RISK ASSESSMENT ESSENTIALS FOR STATE ENERGY SECURITY PLANS

April 2024

U.S. DEPARTMENT OF ENERGY
Office of Cybersecurity, Energy Security, and Emergency Response

This document was produced by the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to aid states in the development of State Energy Security Plans (SESPs). States are encouraged to adapt or supplement the provided material as needed to better align with existing state roles, authorities, and plans to better address state-specific needs and situations. This document is not intended to be prescriptive or suggest non-statutory expansion of State Energy Office responsibilities.

Acknowledgement

The Risk Assessment Essentials for State Energy Security Plans was developed by DOE CESER with funding from the U.S. Department of Energy's State Energy Program in the Office and State and Community Energy Programs. Review and comments were provided by staff from Pacific Northwest National Laboratory (PNNL) and the National Association of Energy Officials (NASEO).

Disclaimer

Acknowledgement 2

Introduction 4

Risk Assessment Framework 5

- Threat 7
- Vulnerability 7
- Consequence 8
- Risk Assessment Template 8

Step 1: Define Risk Scenarios 10

Step 2: Identify Key Stakeholders 11

Step 3: Engage Key Stakeholders 13

- Approaches to Stakeholder Engagement 13
- Stakeholder Engagement Best Practices 13
- Stakeholder Questions 14

Step 4: Develop Risk Problem Statements 15

Step 5: Calculate Risk Scores 16

- Assessing Component Scores 16
- Calculating Risk Scores 20
- Graphical Risk Matrix 21
- Documenting the Risk Assessment 22

Appendix A. Common Threats Included in Risk Assessment 23

Appendix B. Cross-Sector Interdependencies 24

Appendix C. U.S. Threat Data Resources 24

Appendix D. Energy Infrastructure Geospatial Data Resources 27

Introduction

Assessing risk to energy infrastructure is a complex, ever evolving, and continuous process involving many different stakeholders and systems.

Understanding risks to energy infrastructure (natural or human-made) allows decision-makers to focus resources on enhancing energy security, reliability, and resilience.

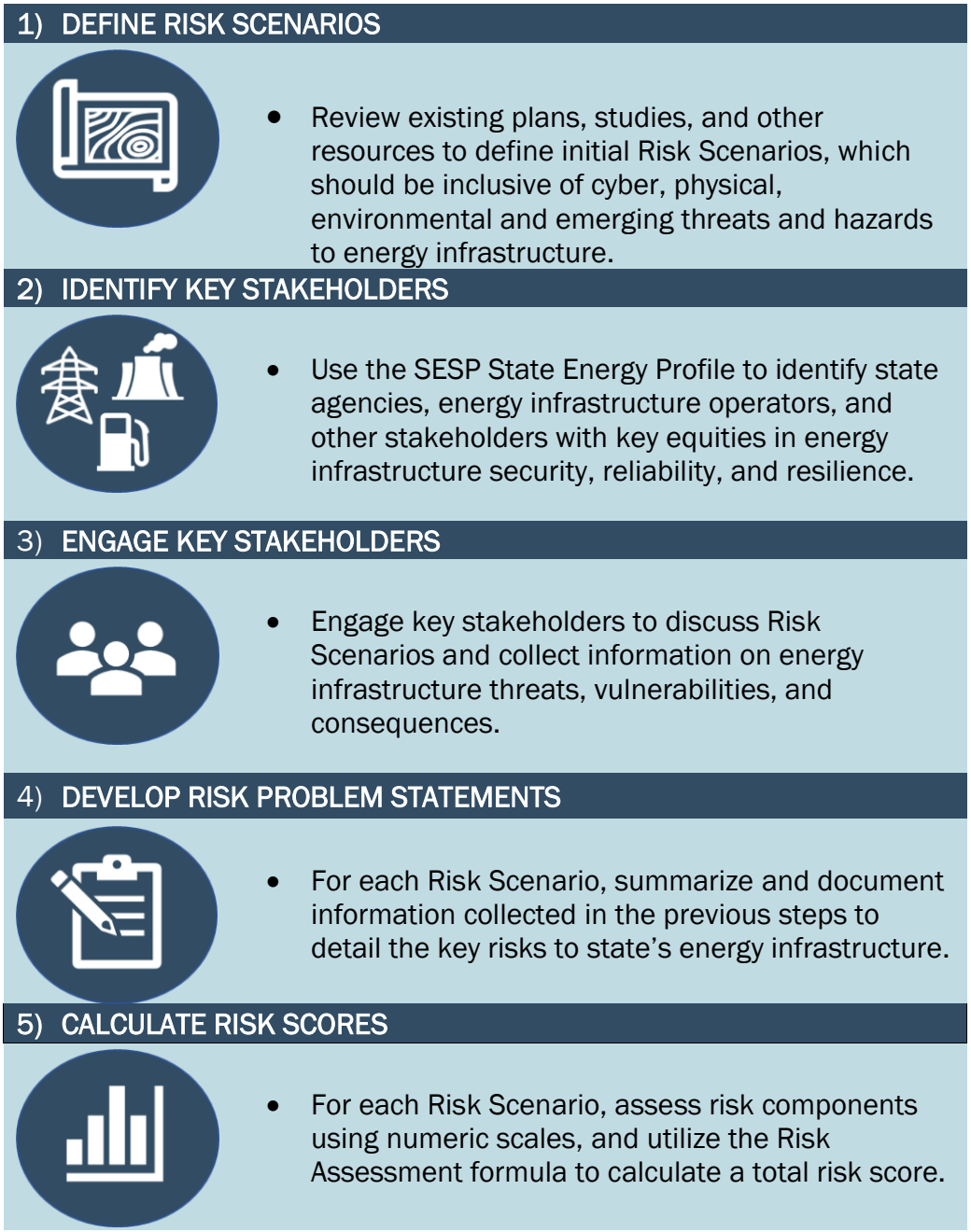
Section 40108 of the Bipartisan Infrastructure Law (BIL) requires that each state and territory have a State Energy Security Plan (SESP), the purpose of which is to ensure reliable, resilient, and secure energy infrastructure (find more information on CESER's State Energy Security Planning Resource page). Each SESP has required elements including: "provide a risk assessment of energy infrastructure and cross-sector interdependencies." One important end goal of the Risk Assessment is to inform the Risk Mitigation Approach (another element required by Section 40108), which outlines a strategy to enhance the reliability and resilience of energy assets. Risk Assessments can also be used to inform emergency preparedness activities, including energy emergency exercises and energy emergency response plans.

There are a range of Risk Assessment methodologies that can be employed to meet the SESP requirements, and when well-designed and thoughtfully implemented, many approaches have the potential to deliver useful results. An ideal methodology should meet the decision-makers' needs and be defensible, transparent, and practical to conduct. Some Risk Assessment methodologies involve significant data collection, analysis, and processing to produce highly quantitative risk ratings. Highly quantitative approaches can provide tremendous insight into energy sector risks and can be powerful decision-making tools for comparing risks and evaluating the benefits of Risk Mitigation measures. However, these approaches often require significant time and resources to execute.

The purpose of this guidebook is to provide a simplified approach to energy infrastructure Risk Assessment that leverages review of existing resources and engagement with energy sector stakeholders to identify, characterize, and assess key risks to energy infrastructure and cross-sector interdependencies.

The suggested steps to develop a simplified Risk Assessment are summarized in **Error! R eference source not found.** and each of these steps is discussed further in subsequent sections of this guidebook.

Exhibit 1. Risk Assessment Steps



Risk Assessment Framework

Energy infrastructure risk is defined as the potential for the loss or degradation of energy supply or services and the associated secondary impacts of those losses on society that result from the exposure of energy infrastructure to a threat. Each risk is specific to a "Risk Scenario"—a hypothetical situation comprising of a threat (e.g., flooding or extreme heat) and an energy infrastructure asset (e.g., electric power substation) or system (e.g.,

electric transmission and distribution network) impacted by that threat. Risk is a function of the magnitude and likelihood of a threat, the vulnerability of the energy infrastructure asset or system to that threat, and the resulting consequences to energy supply and services from the loss or degradation of the energy infrastructure asset. Exhibit 2 presents the Risk Assessment formula and defines each of the key components of the risk equation. The risk formula and definitions presented below are consistent with the DHS Risk Lexicon (2010), however the risk definitions have been adapted for the energy sector.

Exhibit 2. Risk Assessment Formula and Key Definitions

THREAT	VULNERABILITY	CONSEQUENCE	RISK
Anything that can damage, destroy, or disrupt energy systems, including natural, technological, human/ physical, and cyber-security events.	The susceptibility of an energy infrastructure system to damage, loss, or degradation caused by a threat due to weaknesses within the system or due to the system's dependence on critical supporting systems or material, technical, or workforce resources affected by the threat.	The effect of the loss or degradation of an energy infrastructure asset on energy supply or service, and the associated indirect impacts of those losses on society.	The potential for the loss or degradation of energy supply or services, and the associated indirect impacts of those losses on society, resulting from the exposure of energy infrastructure to a threat.

This formula is important to understand conceptually. As any one of the risk components increases, the resulting Risk Score will increase by the same factor as the increase in the risk component. For example, within a Risk Scenario for a hurricane threat to the state's electrical transmission and distribution system, if the probability or likelihood of the hurricane threat was doubled, the Risk Score could be doubled as well (if all other variables are constant). Similarly, a mitigation project that reduces the vulnerability of the transmission network by half (e.g., by reinforcing utility poles) would halve the resulting Risk Score.

THREAT

A "threat" refers to anything that can damage, destroy, or disrupt energy systems, including natural, technological, human/physical, and cybersecurity threats. Examples of natural threats can include natural hazards such as hurricanes, earthquakes, extreme cold, extreme heat, drought, wildfires and ice storms. Human/physical threats include cyber attacks, acts of trespassing or vandalism, as well as more serious acts, such as deliberate attacks or sabotage using ballistics, explosives, or other means. (*See Appendix A. Common Threats Included in Risk Assessment**Error! Reference source not found.***). A threat assessment should attempt to incorporate both historic event data as well as forward-looking projections on how threat probabilities may increase or decrease in the future.

Each threat may be defined using quantitative and/or qualitative metrics. For example, "extreme cold" may be defined as average temperatures dropping below 10 degrees Fahrenheit for a period of 24 hours or longer. The definitions of some threats may vary regionally based on the design standards of infrastructure in that region. For example, the threshold for "extreme cold" in Minnesota may be much lower than the threshold for "extreme cold" in Texas, as equipment in each state is designed to withstand a different temperature threshold. If appropriate, some threats may be further segmented by intensity or severity. For example, a hurricane threat may be segmented by storm strength (e.g., category 3 (111-129 mph winds), category 4 (130-156 mph winds), and category 5 (157+ mph winds).

VULNERABILITY

"Vulnerability" refers to the susceptibility of an energy infrastructure system to damage, loss, or degradation caused by a threat due to weaknesses within the system, or due to the system's dependence on critical supporting systems or material, technical, or workforce resources affected by the threat. Vulnerabilities may be specific to the threat, energy type, and infrastructure asset type/component given the asset's design and its critical dependencies and interdependencies. For example, electric power substations located at ground level may be more vulnerable to flooding than pole- or tower-mounted electric power transmission lines, which are elevated and less likely to be directly impacted by rising waters.

When assessing vulnerability, consider both dependencies (linkages or connections between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other) and interdependencies (bidirectional relationships between two infrastructures) where the state of each infrastructure influences or is reliant upon the state of the other.[1] As an example of a dependency, a buried petroleum pipeline may have a low

[1] Rinaldi, S M, Peerenboom, J P, Kelly, T K, and Decision and Information Sciences. "Identifying, understanding, and analyzing critical infrastructure interdependencies," in IEEE Control Systems Magazine, vol. 21, no.6, pp.11-25, Dec 2001,doi:10.1109/37.969131.

vulnerability to direct damage from hurricane winds, but the pipeline's operations may be impacted if pump stations or terminals connected to the system are out of service due to power outages caused by the hurricane winds. Vulnerability assessments may consider both the level of damage to the infrastructure from the threat as well as the availability of resources—including labor, equipment, and critical components or materials—needed to restore or replace the asset or system. Availability of resources may be impacted by several factors, including the number of assets or system elements needing restoration, impacts to roadways and other transportation systems needed to move resources to damage sites, and supply chain issues for critical components or materials.

CONSEQUENCE

"Consequence" refers to the effect of the loss or degradation of an energy infrastructure system or asset, including the "immediate or "direct consequence" and subsequent "indirect consequence." The direct consequence of an energy infrastructure system or asset outage is the loss of energy supply or services (e.g., production, transportation, transmission, or distribution) provided by the asset and may be expressed in units of energy supply (e.g., megawatt hours of electricity, barrels of petroleum products, cubic feet of natural gas) or number of impacted customers. The indirect consequence refers to the cost to society from the loss in energy supply, which may include economic losses, loss of life or human health, loss of dependent infrastructure functionality, loss of customer service, or degradation of public opinion and trust. Not all direct consequences to energy supply will result in indirect consequences to consumers. Indirect consequences are generally harder to estimate and may vary significantly depending on regional and seasonal variation in energy consumption, redundancies in supply or transportation systems, or the availability of energy storage or other resources to offset the loss of energy supply. Diagrams outlining dependencies and interdependencies between the electricity, liquid fuels, and natural gas subsectors, and other critical sectors are provided in *Appendix B. Cross-Sector Interdependencies.*

RISK ASSESSMENT TEMPLATE

For each Risk Scenario considered in the Risk Assessment, it is important to collect specific information on threat, vulnerability, and consequence. This information may be collected in the template provided in Exhibit 3. A completed template is presented in Exhibit 5 in *Step 4: Develop Risk Problem Statements*.

Exhibit 3. Risk Assessment Template

Risk Scenario A: [Threat]/[Energy Asset or System]	
THREAT 	• *Anything that can damage, destroy, or disrupt energy systems, including natural, technological, human/physical, and cybersecurity threats.* • *Probability of occurrence on an annual basis, typically on a scale of 0% to 100%.*
VULNERABILITY 	• *Susceptibility of an energy infrastructure system to damage, loss, or degradation caused by a threat due to weaknesses within the system or due to the system's dependence on critical supporting systems or material, technical, or workforce resources affected by the threat.* • *May be interpreted as the expected outage duration from exposure to a given threat.* • *Typically, specific to asset type and region.* • *Should include interdependency considerations.*
CONSEQUENCE 	• *Specific to asset or system, often based on total energy or number of customers affected.* • *Should consider indirect or secondary consequences to the society, including impacts to critical energy users and/or vulnerable communities.*
RISK 	• ***Overall summary of risk considering threat probability, vulnerability (duration), and consequence of the Risk Scenario.***

Step 1: Define Risk Scenarios

The first step in Risk Assessment is to review existing plans, studies, after action reports, and other resources to define specific Risk Scenarios to include as part of the Risk Assessment. A Risk Scenario (as described in the Framework) is a hypothetical situation comprising of a threat (e.g., flooding, cyber attack, or extreme heat) and an energy infrastructure asset (e.g., electric power substation) or system (e.g., electric transmission and distribution network) impacted by that threat. For example, a review of existing resources may reveal that hurricanes are a major and increasing threat to coastal areas of the state and that past hurricane events have caused significant power outages. Based on this information, a Risk Scenario may be developed that involves the threat of a Category 3 hurricane to the electric grid in the state's coastal region. Other scenarios may be similarly constructed in the Risk Assessment and may vary based on the nature of threats and energy infrastructure in the state. Specific information related to threat, vulnerability, and consequence for each Risk Scenario would be collected during the stakeholder engagement process in Step 3, and additional Risk Scenarios may be identified during this process.

The initial definition of Risk Scenarios may be informed through a review of existing threat resources, including the State's Hazard Mitigation Plan (HMP), Threat and Hazard Identification and Risk Assessment (THIRA), or existing studies from local universities or others. Additional resources for assessing state threats and hazards are listed in *Appendix C. U.S. Threat Data Resources*. Energy infrastructure assets and systems include electric sector assets such as power plants, transmission lines, and substations; petroleum sector assets such as refineries, pipelines, and storage terminals; and natural gas sector assets such as gas processing plants, transmission pipelines, and storage facilities. A full list of energy infrastructure asset and system types, along with resources for geospatial information, is provided in *Appendix D. Energy Infrastructure Geospatial Data Resources.* Not all infrastructure in this Appendix needs to be considered in the Risk Assessment. The scope of the Risk Assessment may be limited to those infrastructure assets or systems whose loss may have a significant consequence to the state. Resources for understanding and assessing the consequence or criticality of energy infrastructure can be identified in the SESP Energy Profile (see outline published at State Energy Security Plan (SESP) Resources hub) or by reviewing other existing studies of state or regional critical energy infrastructure.

Forward Looking Threat Assessment
If conducting an independent threat or hazard assessment, state officials may need to consider the impact of changing climatic conditions on historical probabilities. Approaches to adapt forward-looking climate information to assess threat probabilities may include (but not limited to) the following: 1. Weighting recent years (~10-15 years) more heavily when calculating threat probability over long historical periods. 2. Applying long-term trends to recent threat probability assessments to increase or decrease threat probabilities over time. 3. Using adapted or downscaled results from global climate models as the basis for forecasts.

Conducting an Energy Infrastructure Threat Assessment
If no existing threat assessment resources exist, an independent assessment may be conducted by analyzing climate data from various government sources (NOAA, USGS, etc.) and mapping those threats against energy infrastructure. GIS data sources for energy systems and assets can be found in *Appendix D. Energy Infrastructure Geospatial Data Resources*, and threat data sources can be found in *Appendix C. U.S. Threat Data Resources*. If conducting an independent threat assessment, it may be important to consider the impact of changing climates on historical threat probabilities. The White House Office of Science and Technology Policy's (OSTP) March 2023 guide on Selecting Climate Information to Use in Climate Risk and Impact Assessments provides high-level guidance on selecting resources (e.g., data, tools, reports, case studies) for understanding climate threats, with a particular focus on understanding exposure to current and future climate-related threats and their potential impacts.

Step 2: Identify Key Stakeholders

After defining Risk Scenarios, key energy sector stakeholders should be engaged to build on the existing knowledge and understanding of risk. Key energy sector stakeholders may include state agencies and regulators, energy infrastructure operators, and others with equities in strengthening energy infrastructure security, reliability, and resilience. The exact number and selection of stakeholders will vary from state to state based on the structure of the state government and specific Risk Scenarios being assessed. Before engaging private sector entities, it is encouraged to review and discuss Risk Scenarios with state agencies, especially the state energy office, emergency management agency, the state fusion center, and the public utilities commission. In many states, it may be important to also engage the governor's office and tribal and local governments to include necessary perspectives.

When identifying relevant energy infrastructure owners and operators to engage, a starting point is to review the state's SESP Energy Profile. Relationships between the private sector and government are crucial to effective communication and information sharing; it is important to understand which agencies in your state have existing relationships with energy infrastructure owners and operators before approaching them for information. In states with only a few energy providers or infrastructure operators, it may be feasible to conduct stakeholder interviews with every major operator. In other states, it may be practical to engage directly with only the largest operators while collaborating with local or regional industry groups that represent collections of smaller operators. For example, working with a state petroleum marketers association, which represents sellers and distributors of petroleum products; a state municipal electric association, which represents public power providers; or a critical infrastructure working group convened by a state's emergency management agency may provide sufficient insights to inform the risk assessment.

Exhibit 4. Examples of Potential Risk Assessment Stakeholders

Government	Energy Infrastructure Owners/Operators	Other
• State energy office • State public utilities commission • State emergency management agency • State governor's office • State fusion center • U.S. Department of Energy (DOE) • U.S. Army Corps of Engineers • U.S. Coast Guard • State National Guard • Local governments • Tribal governments • State public health agency • U.S. Department of Homeland Security, Cybersecurity, Infrastructure Security Agency (DHS CISA) security advisors • U.S. Department of Defense (DOD)	• Investor-owned utilities • ISO/RTOs • Rural and municipal electric association • Rural electric cooperatives • Municipal utilities • Independent power producers • Petroleum marketers association • Petroleum pipeline operators • Petroleum terminal Operators • Petroleum refiners • Natural gas association • Natural gas pipeline operators • Natural gas local distribution companies (LDCs) • LNG terminal operators • Propane marketers association • Heating oil distributors • Retail fuel sellers • Port operators • Rail operators	• National Association of State Energy Officials (NASEO) • National Association of Regulatory Utility Commissioners (NARUC) • Local universities/colleges • Critical energy consumers (e.g., hospitals, water treatment facilities) • Airport fuel farm operators • Trade organizations • Military bases

Step 3: Engage Key Stakeholders

After key stakeholders have been identified, the next step is to engage these stakeholders to discuss the Risk Scenarios defined in Step 1 and to gather relevant information about energy infrastructure risk, including information on threats, energy infrastructure vulnerabilities, and the consequences of energy infrastructure outages.

APPROACHES TO STAKEHOLDER ENGAGEMENT

There are various approaches to engage stakeholders including:

- **Group meetings** allow for engagement with multiple stakeholders (either virtual or in-person) at the same time. Group meetings are particularly effective for communicating information out to multiple parties but may be less effective at gathering information from industry due to general reluctance by industry to discuss challenges in an open forum.
- **Individual stakeholder interviews** offer the opportunity to gather company-specific information, ask follow-up questions as needed, and generally allow for more in-depth discussions in a closed setting. Conducting individual interviews can be time consuming, depending on the number of interviews, and can take longer to identify contacts and schedule.
- **Questionnaires facilitate** the collection of a consistent set of information from multiple entities with a relatively low level of time and effort. Significant time and care may be needed to design survey questions to capture clear and consistent responses. While this approach works well for specific, well-framed questions, it may limit the depth of information collected. Surveys may include a mix of question types (e.g., multiple choice, rating scale) to capture responses in a variety of formats but may require open-ended fields to allow stakeholders to clarify or expand on their responses.

The approaches above are not mutually exclusive, and stakeholder engagement often works best when multiple approaches are utilized. For example, a successful engagement may start with several stakeholder group meetings (e.g., for electric utilities, petroleum marketers) to explain the goals of the Risk Assessment. To emphasize the importance of the effort to energy infrastructure owners and operators, high-ranking government officials may be invited to make remarks, such as representatives from the governor's office, public utility commissioners, or members of the emergency management agency. The group meetings may be followed up with surveys to quickly gather specific and consistent information related to the Risk Assessment from multiple parties. Finally, individual interviews may be scheduled with larger infrastructure operators to gather more details or supplement the information collected through the surveys.

STAKEHOLDER ENGAGEMENT BEST PRACTICES

The following best practices are recommended to ensure that efforts to engage and gather information from stakeholders are successful:

- **Leverage existing contacts across the state government to set up engagements with energy infrastructure operators.** Many state agencies already work with energy infrastructure operators, typically in a regulatory fashion. For example, the state public utility commission typically oversees the state's investor-owned electric and natural gas utilities; state environmental agencies may regulate emissions and/or emergency response plans for power plants, refineries, pipelines, and terminal

operators; and the state department of transportation may register HAZMAT vehicles, such as tanker trucks, that distribute petroleum products. Working through state or regional industry groups, such as state petroleum marketers associations, may help facilitate engagements with infrastructure operators in the state.

- **Review publicly available information before engaging stakeholders.** Private sector entities participating in Risk Assessment will typically be doing so on a voluntary basis. State engagements should be focused on gathering information that is not already in the public domain. Reviewing the SESP Risk Profile, company annual reports, or information published by the Energy Information Administration will provide a baseline of understanding and will allow the discussion to focus on non-public information.
- **Explain the purpose of the SESP.** Prior to requesting information from stakeholders, it is important to help stakeholders understand the purpose and necessity of the SESP and the Risk Assessment. This includes describing the goals of SESP, why the stakeholder's participation is important, and how the results of the Risk Assessment may be used to inform energy sector Risk Mitigation strategies that may affect the stakeholder. Furthermore, it may be important to emphasize during initial outreach that the development of the SESP is not a regulatory activity and that participation in the SESP process will not be used to punish or penalize industry.
- **Define key risk terms and rating scales to ensure clarity.** Throughout stakeholder interactions, it is helpful to provide precise definitions of key terms such as 'threat,' 'vulnerability,' and 'consequence'. To the extent that stakeholders provide numeric or non-numeric ratings of risk components, rating scales should be clearly defined to ensure consistency.
- **Use non-disclosure agreements (NDAs) and other protections to assure confidentiality.** Private companies are generally reluctant to share business-sensitive information or information that may provide insight into weakness or vulnerabilities in their systems that could be exploited. It is important to provide assurances to participating companies that information shared with the state will remain confidential and will not be released publicly either intentionally or unintentionally. This may involve the use of non-disclosure agreements (NDAs) and/or the use of legal protections that prevent gathered data or information from disclosure. The National Governors Association published a paper on State Protection of Critical Energy Infrastructure (CEII) that contains some examples of state laws designed to protect this information.

STAKEHOLDER QUESTIONS

Stakeholder interviews should be designed to collect specific information on the threat, vulnerability, and consequence of the Risk Scenarios being considered by the Risk Assessment. Questions for stakeholders may involve a mix of specific questions designed to gather specific information and open-ended questions that allow the stakeholders to discuss broader risk and risk mitigation topics. Discussions with stakeholders may identify additional Risk Scenarios that may be included in the Risk Assessment. Optionally, questions may be asked about potential Risk Mitigation Measures related to the Risk Scenarios under consideration to help inform the SESP Risk Mitigation Approach.

Step 4: Develop Risk Problem Statements

In Step 3, specific information was collected on the threat, vulnerability, and consequence of select Risk Scenarios—hypothetical situations involving specific threats to specific energy infrastructure assets or systems. For each Risk Scenario, this information may be summarized using the Risk Assessment Template (see Exhibit 3) to develop a Risk Problem Statement that clearly describes and details the threat, vulnerability, and consequence of the Risk Scenario. An example of a Risk Problem Statement is presented in Exhibit 5 below. Risk Problem Statements should be developed for each of the Risk Scenarios evaluated as part of the Risk Assessment.

Exhibit 5. Example Risk Problem Statement

Risk Scenario A: 2-foot Flooding /Big State City Substations	
THREAT 	The Big State River in the southern district of Big State City has flooded three times over the past 20 years, including twice in the past 5 years with river levels reaching as high as 1.5 feet above flood stage during the 2021 flood event. Flooding has occurred more frequently in recent years due to new developments impacting stormwater drainage in Big State City and due to more frequent high-precipitation rainfall events. According to current climate projections, heavy rainfall events are expected to occur more frequently in the future, increasing the threat to assets located in the floodplain.
VULNERABILITY 	Current flood prevention measures at Big State Utility's electric power substations in the southern district of Big State City are sufficient to prevent flooding when river levels are up to 2 feet above flood stage. Beyond 2 feet, existing flood prevention measures would be insufficient to protect the facility, which would be severely damaged if fully inundated. Repairs to inundated substation infrastructure would likely take several weeks to fully repair.
CONSEQUENCE 	Big State Utility estimates that 5 of its high-voltage substations (69-kV+) are potentially exposed to the flood threat and that these substations serve a total of approximately 100,000 customers in the southern district of Big State City. Simultaneous loss of all 5 substations would leave about 25% of Big State City without power, including the downtown commercial district and Big State City Hospital, which is the largest of three hospitals in Big State City. Big State City Hospital has an emergency backup generator capable of serving critical facility loads, but this generator can only operate for approximately 48 hours before refueling.
RISK 	**If flooding along the Big State River exceeds 2 feet, existing flood protections could be exceeded at approximately five Big State Utility high-voltage substations that serve the southern district of Big State City, potentially disrupting power supply to the downtown commercial district, including Big State City Hospital.**

Step 5: Calculate Risk Scores

The final step in Risk Assessment is to develop ranks, scores, or tiered ratings for each Risk Scenario using information detailed in the Risk Problem Statements. Calculating Risk Scores allows Risk Scenarios to be compared with one another on a consistent basis, which may help inform the Risk Mitigation Approach and other planning activities. While there are many ways to calculate Risk Scores or ratings, it is important that whatever method used be consistently applied across Risk Scenarios. This guidebook provides a simple approach that:

- Assesses a relative score/rating to each of the three risk components that make up the Risk Assessment formula (threat, vulnerability, and consequence) for each Risk Scenario.
- Calculates a total Risk Score for each Risk Scenario by multiplying the component scores in the Risk Assessment formula (see **Error! Reference source not found.** in the c hapter on *Risk Assessment Framework*).
- Compares the total Risk Scores for each Risk Scenario in a table or Risk Matrix.

This approach may be expanded to include additional risk components, utilize different rating scales or component weightings, or other adjustments that take state-specific situations and priorities into account. For example, some states may choose to expand the consequence component into separate direct and indirect consequence components. Whatever the choice of methodology, any factors, scales, or weightings used should be clearly explained when *Documenting the Risk Assessment*.

ASSESSING COMPONENT SCORES

Assigning scores for each of the key risk components requires the use of clearly defined scales that relate to underlying quantitative metrics (e.g., annual event probability) or qualitative descriptors. Risk scales can correspond to the underlying metrics in various ways, including uniform scales, adjusted uniform scales, and “rough order of magnitude” scales. Examples of three different 5-point threat scales based on underlying annual threat probabilities are shown in Exhibit 6, and the various methods for scaling are discussed below the exhibit. The scales presented in this chapter correspond to underlying metrics, many of which may be difficult to assess with precision. Given the inherent uncertainty in this activity, this guidebook suggests using scales that group Risk Scenarios into tiers that correspond to wide ranges in the underlying metrics.

Exhibit 6. Threat Probability Assessment Using Different Quantitative Scaling Options

Category		Annual Threat Probability (% per year)		
Score	Tier	Uniform Scale	Adjusted Uniform Scale	Rough Order of Magnitude Scale
1	Low	0%-20%	0%-10%	<1%
2	Med-Low	20%-40%	10%-20%	1%-5%
3	Medium	40%-60%	20%-30%	5%-15%
4	Med-High	60%-80%	30%-40%	15%-35%
5	High	80%-100%	>40%	>35%

In Exhibit 6 the uniform scale is perfectly scaled to the maximum value of 100% with each 20% increase in the annual threat probability associated with a one-point or one-level increase on the threat scale. The adjusted uniform scale shown in the exhibit is similar to the uniform scale except the levels are set to allow for more differentiation at lower probabilities (in this case, below 40%), reflecting where the majority of the underlying data lies. How to adjust a uniform scale to fit the underlying data is a matter of judgement. The third approach shown in the exhibit is the rough order of magnitude approach, which uses uneven changes in the threat probability between threat levels. For example, in Exhibit 6, the interval is 1% for Low-Low (<1%), 4% for Medium-Low (1%-5%), 10% for Medium (5%-15%), 20% for Med-High (15%-35%), and 65% for High (>35%). The rough order of magnitude approach is often helpful when the underlying data are hard to estimate precisely (large statistical error bars) or in situations where subject matter experts feel more comfortable providing general "ballparks" given inherent uncertainty of the values being estimated.

Note that relative risk scales have the effect of reducing the difference between the high and low ends of the scale. For example, a threat with a 50% annual probability would by definition occur 100 times more often than a threat with a 0.5% annual probability but would have a threat score only 3 times as high using the uniform scale in Exhibit 6 and 5 times as high using the adjusted uniform or rough order of magnitude scales.

Example assessment scales for vulnerability and consequence are presented in Exhibit 7 and Exhibit 8. Vulnerability scores are expressed in terms of the duration of the infrastructure outage. Consequence scores in Exhibit 8 are expressed in terms of the percentage of state supply or customers experiencing service disruptions.

Exhibit 7. Vulnerability Assessment Using Different Quantitative Scaling Options

Category		Vulnerability (Duration)		
Score	Tier	Uniform Scale (Days)	Adjusted Uniform Scale (Days)	Rough Order of Magnitude Scale
1	Low	0-1	<1	Minutes
2	Med-Low	1-2	1-3	A few hours
3	Medium	2-3	3-7	~1 day
4	Med-High	3-4	7-14	Several days
5	High	5+	14+	1 week+

Exhibit 8. Consequence Assessment Using Different Quantitative Scaling Options

Category		Consequence (Share of State Supply or Customers)		
Score	Tier	Uniform Scale	Adjusted Uniform Scale	Rough Order of Magnitude Scale
1	Low	0%-20%	0%-10%	<1%
2	Med-Low	20%-40%	10%-20%	1%-5%
3	Medium	40%-60%	20%-30%	5%-15%
4	Med-High	60%-80%	30%-40%	15%-35%
5	High	80%-100%	>40%	>35%

If using a quantitative consequence scale as in Exhibit 8, it may be necessary to adjust the scale or add weightings for different energy types, recognizing that different forms of energy will have different indirect impacts on society. For example, the loss of customer electric power service is likely to have a larger immediate impact on society than the loss of petroleum fuels. Alternatively, states may choose to employ a qualitative scale that takes both direct and indirect consequences into account. Exhibit 9 provides an example qualitative scale for consequence scoring that provides descriptions of consequences that account for the extent of the disruption (widespread versus localized) and secondary consequences, such as impacts of the loss of energy supply on lifeline[2] sectors, vulnerable populations, and the economy. Exhibit 9 provides consequence descriptions for each of the main energy types—electricity, liquid fuels, and natural gas. Electricity is further divided between consequences that involve service outages, typically caused by damage to the transmission and distribution lines, and electricity shortages that may involve generation outages or demand spikes that put grid reliability at risk and that may result in rolling blackouts or even grid collapse. The consequence tiers in Exhibit 9 build on one another in that descriptions of consequences in lower tiers carry up to the higher tiers, unless superseded by text in the higher tier descriptions. For example, if "below-average inventories" are mentioned in the tier 3 box, then below-average inventories are also included for tier 4 events even if not explicitly listed in the tier 4 box.

States using any of the example assessment scales presented in this guidebook (particularly Exhibit 9) should adapt these scales to reflect state-specific situations and priorities. **It may be difficult for stakeholders to precisely predict the consequences of a specific Risk Scenario. What matters more than precision is consistently grouping Risk Scenarios into specific tiers.** For consequences that have some elements of a higher tier and some elements of a lower tier, partial scoring may be applied (e.g., 2.5 or 3.5).

[2] A lifeline enables the continuous operation of critical government and business functions and is essential to human health and safety or economic security Community Lifelines | FEMA.gov. Lifeline sectors include safety and security; food, hydration, and shelter; health and medical; energy; communications; transportation; hazardous materials; and water systems. See Appendix B for further information on key dependencies and interdependencies between the energy subsectors (electricity, petroleum, and natural gas) and other lifeline sectors.

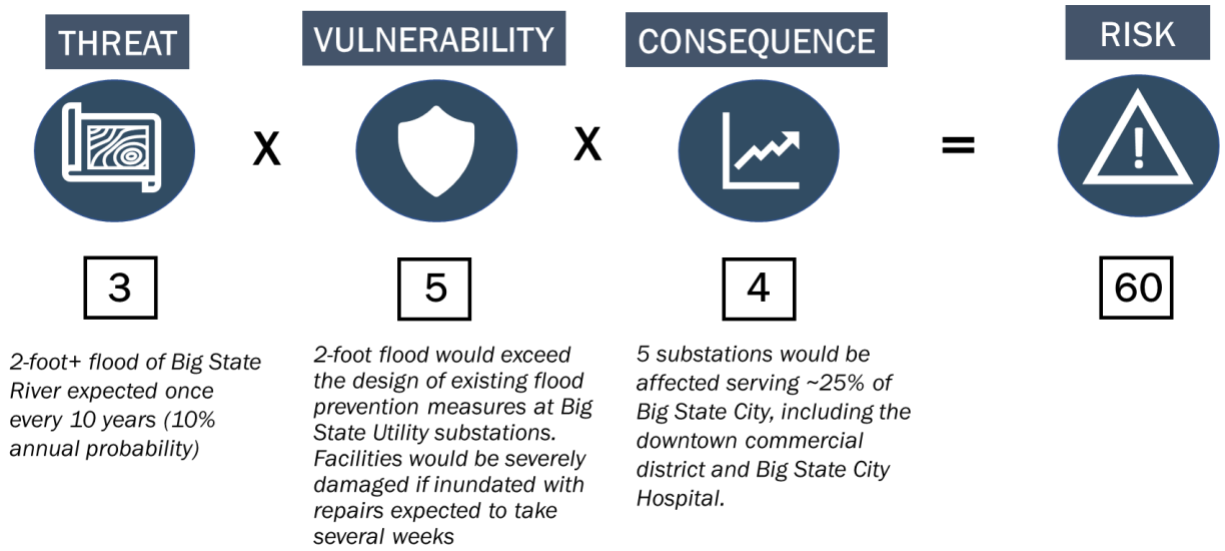
Exhibit 9. Consequence Assessment Using Qualitative Scaling. Note impact may be a result of a natural hazard or human made (cyber or physical attack).

Score	Electricity	Liquid Fuels	Natural Gas
1) Low	• **Service Disruption:** Grid is damaged in places but customers remain supplied as contingency actions allow power to be rerouted to avoid disruption in service.	• Any resulting supply loss offset by storage assets across the transportation and delivery system. Minimal impact to pricing.	• Any resulting supply loss offset by storage assets across the transmission and delivery system. Minimal impact to pricing.
2) Med-Low	• **Service Disruption:** Localized power outages.	• Supply loss offset by storage assets but prices see notable increase.	• Supply loss offset by storage assets but prices see notable increase.
3) Medium	• **Service Disruption:** Widespread but temporary power outages affecting a major metropolitan area or region of the state. • Lifeline sectors largely maintained with backup generators. • **Electricity Shortage:** Loss of generation leads to significant reduction in operating reserves, but reserves remain above thresholds for emergency action.	• Sporadic fuel outages and delivery delays impacting end users (e.g., gas stations, heating customers) as supply and distribution do. • Infrastructure struggles to keep up with sudden spike in demands. • Localized supply shortages at bulk terminals. Distributors begin loading trucks at terminals further away to meet customer needs. • Local or regional fuel inventories fall near or below the bottom of previous five-year range.	• Major transmission pipeline issues Operational Flow Orders (OFOs) to avoid system strain. Usually driven by high-demand cold periods or infrastructure outages or constraints. • High local or regional prices versus U.S. benchmarks may indicate issues. • High prices in affected markets lead to voluntary fuel switching for power sector and industrial customers with the ability to switch.
4) Med-High	• **Service Disruption:** Widespread power outages affecting a major metropolitan area or region of the state. • Lifeline sectors experience temporary or intermittent disruptions as backup generator fuel is exhausted and awaits replenishment. • Vulnerable groups that rely on electricity moved to shelters or provided backup generators as needed. • **Electricity Shortage:** Grid operators issue emergency alerts for critical conservation and to maximize generation and transmission resource availability. Sharp price spikes across balancing areas.	• Widespread run-outs and/or delivery delays for end users and bulk terminals as suppliers cannot meet all demands. • Typically associated with extended outage of one or more critical supply assets. • Sharp declines in local or regional fuel inventories to well below previous five-year lows. • Sharp price spreads versus U.S. or international benchmarks may indicate significant regional issues.	• A major transmission pipeline has an extended unplanned outage during a (local or regional) peak demand period. • Some gas is rerouted into the region on alternate pipelines, but due to capacity constraints, supply is interrupted to power plants and other customers with non-firm contracts. • Local distribution companies (LDCs) urge customers to conserve gas use. • Gas supply disruptions to power generators reduce available generation resources, forcing grid operators to issue emergency advisories or alerts.
5) High	• **Service Disruption:** Widespread power outages affecting a major metropolitan area or region of the state. • Lifeline sectors, including Emergency Response, experience severe impacts from difficulty refueling vehicles and backup generators due to impact of power outages on liquid fuels supply chains. • **Electricity Shortage:** Grid operators initiate rolling blackouts to preserve grid stability. Typically associated with large-scale loss of generation resources due to power plant operational outages or power plant fuel shortages.	• Fuel unavailable or inaccessible to most end users as widespread power outage or other common event renders retail outlets and critical supply infrastructure inoperable. • Lifeline sectors, including Emergency Response, have difficulty finding supply, impacting provision of essential services. • Vulnerable groups that rely on propane/heating oil moved to shelters.	• Severe outage/damage or supply shortage forces transmission pipelines and LDCs to interrupt supply to firm customers. • Loss of pressure in the gas distribution system causes gas to be shut off to firm customers (residential and commercial) • Restoring service is time-consuming, as the LDC must relight each customer's pilot light. • Vulnerable groups dependent on gas heating moved to shelters. • Loss of gas-fired generation leads to severe regional electricity shortages. Grid operators initiate rolling blackouts to preserve grid stability.

CALCULATING RISK SCORES

Once component scores have been assessed for each of the Risk Scenarios under evaluation, these scores may be multiplied using the risk formula to produce a total Risk Score. Exhibit 10 presents an example of the Risk Assessment calculation using 5-point numeric scales for threat, vulnerability, and consequence values, where 1 is the lowest value and 5 is highest value. Note that the scores and calculations presented in this exhibit are for explanatory purposes only.

Exhibit 10. Relative Risk Formula Example: 2-foot Flooding /Big State City Substations



In Exhibit 10, the threat score (3) indicates a medium probability event—in this case one that occurs once every 10 years; the vulnerability score (5) indicates high expected damage to the infrastructure asset or system (in this case an outage lasting more than a week); and the consequence score (4) indicates that the loss of the energy asset would have a medium-high impact on society, including outages affecting 25% of Big State City, including impacts to a major hospital. Multiplying each of these components together produces a total Risk Score of 60. This score can then be compared to similarly constructed Risk Scores for other Risk Scenarios to understand relatively which risks are larger or smaller. Exhibit 11 presents an example of risk calculations for various Risk Scenarios using different component (threat, vulnerability, and consequence) scores. Note that these scores and calculations are presented for explanatory purposes only.

Exhibit 11. Risk Score Calculations for Various Risk Scenarios

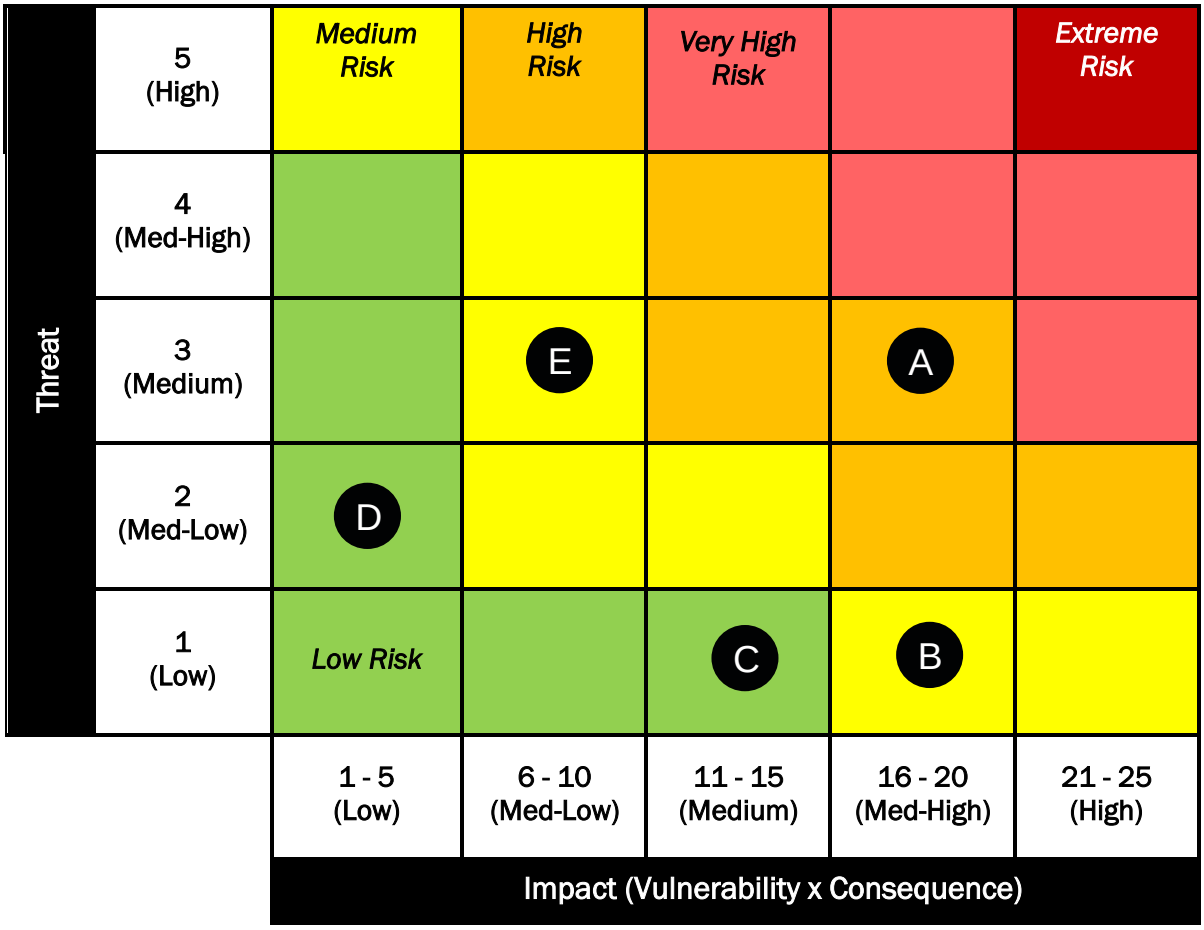
Risk Scenario (Threat/Infrastructure)	Threat	Vulnerability	Consequence	Risk
A. 2-foot Flooding /Big State City Substations	3	5	4	**60**
B. Cat. 3 Hurricane/Big State Transmission Lines	1	4	5	**20**
C. 8.0 M Earthquake/Big State Petroleum Pipeline	1	5	3	**15**
D. Wildfire/Big State Gas Storage Facility	2	2	1	**4**
E. Extreme Cold/Big State Basin Oil & Gas Wells	3	3	3	**27**

Exhibit 11 shows a range of Risk Scores with Scenario A resulting in the highest overall risk score (60). The risk scores in this table can be compared with one another on a relative basis—for example, Scenario A is relatively three times as large as Scenario B and four times as large as Scenario C.

GRAPHICAL RISK MATRIX

Graphical presentation of the Risk Assessment results through charting or mapping is a useful way to analyze risk results and recognize trends and patterns to help draw Risk Assessment conclusions. One method of analyzing and visualizing risk is to develop a Risk Matrix (sometimes called a heat map) to show how Risk Scenarios compare to one another along two key variables: threat (probability) and "impact" (a combination of vulnerability and consequence). Exhibit 12 presents an example of a Risk Matrix.

Exhibit 12. Illustrative Risk Matrix with Risk Scenarios Plotted



The example Risk Matrix in Exhibit 12 plots the impact score—comprised of the vulnerability score multiplied by the consequence score—on the x-axis and the threat score—associated with probability—on the y-axis. In this example, the x-axis is rated on a scale of 1 to 25 and the y-axis is rated on a scale of 1 to 5, but more granular rating scales may be applied. Generally, scenarios that are plotted closer to the upper right-hand corner of the Risk Matrix will have the higher risk scores. The color-coding of the cells in the Risk Matrix indicate five risk categories based on the intersection of the threat and impact scores: extreme, very high, high, medium, and low, with each risk category covering a range of Risk Scores. The

example Risk Matrix in Exhibit 12 plots the five Risk Scenarios from Exhibit 11. Note that these scores are presented for explanatory purposes only.

DOCUMENTING THE RISK ASSESSMENT

The results of the SESP Risk Assessment should be documented in the SESP. An example outline for documentation is provided in Exhibit 13.

Exhibit 13. Risk Assessment Outline

Section	Content
1. Risk Assessment Approach	• List of reports, datasets, and other resources utilized • List of key stakeholders consulted • Documentation of risk scoring methodology, including any formulas, rating scales, and weightings used
2. Inventory of Risk Problem Statements	• See *Exhibit 3. Risk Assessment Template*
3. Risk Assessment Results	• Table of Risk Score calculations (see Exhibit 11) • (Optional) Graphical Risk Matrix (see Exhibit 12)

Appendix A. Common Threats Included in Risk Assessment

Threat	General Description
Attack (Cyber)	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of energy infrastructure assets, including attacks targeting information technology (IT) and operational technology (OT) systems.
Attack (Physical)	A deliberate attack or sabotage using kinetic means (firearms, explosives, drones, vehicles, etc.) on any part of an energy system.
Winter Storm (Blizzard)	Events in which the main types of precipitation are snow, sleet, or freezing rain.
Drought	A deficiency of precipitation over an extended period of time resulting in a water shortage.
Earthquake	Shaking of the Earth's surface by energy waves emitted by slowly moving tectonic plates overcoming friction with one another underneath the Earth's surface.
Extreme Cold (Cold Wave)	A rapid fall in temperature within 24 hours and extreme low temperatures for an extended period.
Extreme Heat (Heat Wave)	A period of abnormally hot weather typically lasting two or more days with temperatures outside the historical averages for a given area.
Flooding (Coastal)	When water (usually saltwater) inundates or covers normally dry coastal land as a result of high or rising tides or storm surges.
Flooding (Riverine)	When streams and rivers exceed the capacity of their natural or constructed channels to accommodate water flow and water overflows the banks, spilling out into adjacent low-lying, dry land.
Hail	A form of precipitation that occurs during thunderstorms when raindrops, in extremely cold areas of the atmosphere, freeze into balls of ice before falling towards the Earth's surface.
Hurricane/Tsunami	A tropical cyclone or localized, low-pressure weather system that has organized thunderstorms but no front (a boundary separating two air masses of different densities) and maximum sustained winds of at least 74 mph.
Ice Storm	A freezing rain situation (rain that freezes on surface contact) with significant ice accumulations of 0.25 inches or greater.
Landslide	The movement of a mass of rock, debris, or earth down a slope.
Lightning	A visible electrical discharge or spark of electricity in the atmosphere between clouds, the air, and/or the ground often produced by a thunderstorm.
Solar Radiation Storms	When a large-scale magnetic eruption, often causing a coronal mass ejection and associated solar flare, accelerates charged particles in the solar atmosphere to very high velocities.
Strong Wind	Damaging winds, often originating from thunderstorms, that are classified as exceeding 58 mph.
Tornado	A narrow, violently rotating column of air that extends from the base of a thunderstorm to the ground and is visible only if it forms a condensation funnel made up of water droplets, dust, and debris.
Volcanic Activity	Occurs via vents that act as a conduit between the Earth's surface and inner layers, and erupt gas, molten rock, and volcanic ash when gas pressure and buoyancy drive molten rock upward and through zones of weakness in the Earth's crust.
Wildfire	Unplanned fire burning in natural or wildland areas such as forests, shrublands, grasslands, or prairies.

Sources: FEMA National Risk Index, NOAA, CESER OE-417

Appendix B. Cross-Sector Interdependencies

CESER has published *Cross-Sector Interdependency Diagrams* on its State Energy Security Plan (SESP) Resources hub. The diagrams show key dependencies and interdependencies between the energy subsectors (electricity, petroleum, and natural gas) and other critical lifeline sectors. States may customize or supplement these diagrams by providing specific examples of cross-sector interdependencies, particularly those that may be affected by the Risk Scenario being assessed, or by discussing the cascading consequences of interconnected energy systems within the state.

Appendix C. U.S. Threat Data Resources

When assessing threats for the energy infrastructure Risk Assessment, it is important to collect information on historic threat frequency and probability, identify areas of threat exposure, and consider forward-looking assessments of how threat probability and exposure may evolve in the future. General resources for this information include:

- State/Local Hazard/Multi-Hazard Mitigation Plans (SHMP)
- State/Local Climate Impact Assessments, Climate Adaptation Plans
- State/Local Emergency Management Plans
- State/Local Energy Emergency Plans
- Threat and Hazard Identification and Risk Assessment (THIRA)
- Annual Threat Assessment of the U.S. Intelligence Community
- State and Regional Energy Risk Profiles | Department of Energy
- NASA SEDAC Hazards Mapper (columbia.edu)
- Events | Billion-Dollar Weather and Climate Disasters | National Centers for Environmental Information (NCEI) (noaa.gov)
- State Climate Summaries 2022 (ncics.org)
- States At Risk: America's Preparedness Report Card | States at Risk

In addition to the resources provided above, the following table provides a list of geospatial hazard layers for specific threats from Federal Emergency Management Agency (FEMA), National Oceanographic and Atmospheric Administration (NOAA), U.S. Geologic Survey (USGS), U.S. Forest Service (USFS), and other agencies and authorities. Resources and techniques for assessing forward-looking threats are included in the *Forward-Looking Threat Assessment* section.

Exhibit 9. Threat Open Data/Description Sources

Threat	Sources	Frequency	Susceptible Area
Avalanche	National Risk Index (NRI) - Avalanche		✓
	Avalanche.org		✓
	Spatial Hazard Events and Losses Database for the United States (SHELDUS)	✓	
Coastal Flooding	National Risk Index (NRI) – Coastal Flooding		✓
	FEMA National Flood Hazard Layer		✓
	National Storm Surge Risk Flood Map		✓
	National Hurricane Center		✓
	Hazus | FEMA.gov		✓
	NOAA Sea Level Rise Viewer and Data How to Calculate Coastal Flood Frequency (noaa.gov)	✓	✓
	State/Local Flood Threat Mapping		✓
Cold Wave/ Extreme Cold	National Risk Index (NRI) – Cold Wave		✓
	National Weather Service (NWS) Iowa Environmental Mesonet	✓	
Cybersecurity	National Cyber Awareness System Cybersecurity Alerts & Advisories SLTTGCC Compendium of Cyber Resources	✓	
Drought	National Risk Index (NRI) - Drought		✓
	US Drought Mitigation Center	✓	
Earthquake	National Risk Index (NRI) - Earthquake		✓
Hail	National Risk Index (NRI) - Hail		✓
	Storm Prediction Center Maps, Graphics, and Data Page (noaa.gov)	✓	
Heat Wave/ Excessive Heat	National Risk Index (NRI) – Heat Wave		✓
	National Weather Service (NWS) Iowa Environmental Mesonet	✓	
Hurricane	National Risk Index (NRI) - Hurricane		✓
	National Hurricane Center Data Archive	✓	
	National Storm Surge Risk Flood Map		✓
	Hazus | FEMA.gov		✓

	Sea, Lake, and Overland Surges from Hurricanes (SLOSH) (noaa.gov)		✓
	Storm Events Database | National Centers for Environmental Information (noaa.gov)	✓	
Ice Storm	National Risk Index (NRI) – Ice Storm		✓
	USACE Damaging Ice Storm GIS	✓	
Landslide	National Risk Index (NRI) - Landslide		✓
	USGS Landslide Hazards Program Preliminary Landslide Susceptibility Maps and Data for Hawaii Puerto Rico Landslide Susceptibility Map		✓
	Cooperative Open Online Landslide Repository (COOLR) project	✓	
Lightning	National Risk Index (NRI) - Lightning		✓
	NCEI Lightning Products and Services		✓
Physical Security	Electricity Information Sharing and Analysis Center (E-ISAC) Oil and Natural Gas Information Sharing and Analysis Center (E-ISAC) State Fusion Centers	✓	✓
Riverine Flooding	National Risk Index (NRI) – Riverine Flooding		✓
	Hazus | FEMA.gov		✓
	FEMA National Flood Hazard Layer		✓
	NCEI Storm Events Database	✓	
Strong Wind	National Risk Index (NRI) – Strong Wind		✓
	Storm Prediction Center Maps, Graphics, and Data Page (noaa.gov)	✓	
Tornado	National Risk Index (NRI) - Tornado		✓
	Storm Prediction Center Maps, Graphics, and Data Page (noaa.gov)	✓	
Tsunami	National Risk Index (NRI) - Tsunami		✓
	State of California, Department of Conservation, Official Tsunami Inundation Maps Hawaii Statewide GIS Program, Tsunami Evacuation Zones Oregon Department of Geology and Mineral Industries, Tsunami Inundation Zones		✓

	Washington State Department of Natural Resources, Tsunami Inundation Data Alaska Department of Natural Resources, Tsunami Inundation Maps Puerto Rico Seismic Network, Tsunami Evacuation Zones Pacific Islands Ocean Observing System (PacIOOS), NEOWAVE Regional Tsunami Model Maps		
	NCEI/WDS Global Historical Tsunami Database	✓	
Volcanic Activity	National Risk Index (NRI) – Volcanic Activity		✓
	UN Office for Disaster Risk Reduction, Volcano Population Exposure Index		✓
	Volcanoes of the World Database	✓	
Wildfire	National Risk Index (NRI) - Wildfire		✓
	"Wildfire Risk to Communities Burn Probability - U.S. Forest Service"		✓
Winter Weather/Storm	National Risk Index (NRI) – Winter Weather		✓
	National Weather Service (NWS) Iowa Environmental Mesonet	✓	

Appendix D. Energy Infrastructure Geospatial Data Resources

The resources provided in this appendix may be useful when mapping energy infrastructure against various threats as part of an optional quantitative threat assessment. If conducting a quantitative threat assessment, it is not necessary to map every infrastructure asset; some may choose to focus assessment on select infrastructure types, infrastructure assets above a specific size or throughput threshold, or assets already determined to be critical based on previous analysis or discussion with stakeholders.

Publicly available geospatial data on energy infrastructure is available to states primarily via:

- Energy Infrastructure and Resources Maps | U.S. Energy Atlas (eia.gov)
- Homeland Infrastructure Foundation-Level Data (HIFLD)

These sources provide locational data and in some cases capacity and operating data for various infrastructure types for all U.S. states and several territories.

Exhibit 8 provides a summary of GIS resources for various energy infrastructure types, including links to datasets. Additional mapping resources maintained by state agencies, utility/energy supplier websites, or private data providers may also be used. When reviewing datasets, it is important to consider the granularity of the dataset, whether the dataset contains ownership and operational details, and when the dataset was last updated.

Exhibit 8. Energy Infrastructure Asset Geospatial Resources

Sector/ Asset Type	Data Source(s)	Description
Electricity		
Power Plants	EIA HIFLD	All operable electric generating plants by energy source with a combined nameplate capacity of 1 megawatt or more that are operating, are on standby, or out of service for short- or long-term.
Wind Generators	USWTDB	U.S. wind turbine database showing the density of wind turbines across the United States.
Transmission Lines	EIA HIFLD	Electric transmission lines varying from 69 kV to 765 kV. Underground transmission lines included where sources were available.
Substations	HIFLD Secure	(*Request Access) ISO Maps – usually pdf.* Electricity substations filtered to the state.
Distribution Lines and Substations	PUC/PSC or utility maps	Distribution system maps/filings. These maps are usually filed with the PUC/PSC but are marked as Critical Energy Infrastructure Information.
Natural Gas		
Interstate and Intrastate Natural Gas Pipelines	EIA HIFLD	Natural gas interstate and intrastate pipelines in the United States.
	NPMS	Natural gas interstate and intrastate pipelines in the United States. Public version available at county level. Request Access for non-public version that provides more detail.
Gas Pipeline Compressor Stations	HIFLD	Locations of natural gas compressor stations by pipeline company.
Distribution and Gathering Pipelines	PUC/PSC or utility maps	Distribution system maps/filings. These maps are usually filed with the PUC/PSC but are marked as Critical Energy Infrastructure Information.
Peak Shaving Facilities	HIFLD	Locations of peak shaving facilities with owner name and number of tanks.
Natural Gas Underground Storage	EIA	A map of U.S. underground natural gas storage facilities showing their locations, ownership, and gas capacity.
Above Ground LNG Storage	HIFLD	Above-ground LNG storage facilities by operator name. This map also includes the street address and how the LNG is transported to the facility.
LNG Import Terminals	EIA HIFLD	Locations of LNG import terminals with facility name, owner, and storage capacity in billion cubic feet.
Natural Gas Processing Plants	EIA	Processing plants in the U.S. showing the capacity and flow of natural gas for each facility.
Natural Gas Wells	HIFLD	Gas production well heads locations as maintained by each state department.
Petroleum		
Petroleum Refineries	EIA HIFLD	Locations of petroleum refineries in the U.S. with site name, corporation, and company.

Product Terminals	EIA HIFLD	Petroleum terminals by company and city name.
	State Title V Filings	State and local environmental agencies may issue and monitor the compliance of Title V air emissions operating permits under the Clean Air Act for petroleum product terminals that meet criteria as "major" emissions sources.
Product Pipelines	EIA	Petroleum pipelines in the United States and their operators.
	NPMS	(Request Access or use public version)
Pipeline Pump Stations	HIFLD	Pipeline pump station locations, including the owner/operator and commodity type.
Petroleum Ports	EIA	Locations of ports that handle greater than 200,000 short tons per year in total volume of petroleum products.
Petroleum Waterways	EIA	Map of waterways that move greater than 700,000 short tons per year of petroleum products.
Crude Oil Pipelines	EIA	Map of crude oil pipelines in the United States.
	NPMS	(Request Access or use public version)
Crude Oil Rail Terminals	EIA	Locations of crude oil rail terminals with description of the station type and whether the terminal is used for loading or unloading.
Oil Wells	HIFLD	Gas production well heads with the name, status, and operator of the wells.
NGLs / Propane		
NGL Pipelines	EIA HIFLD	Hydrocarbon gas liquid pipelines by operator name and pipeline name.
	NPMS	Natural gas interstate and intrastate pipelines in the United States. Public version available at county level. Request Access for non-public version that provides more detail.
Propane Terminals		Source-specific research.
NGL Fractionators		Source-specific research.
Underground Propane Storage		Source-specific research.
Other		
Coal Mines	EIA	Locations of coal mines with a description of whether the mine is underground or surface level.
Ethanol Plants	EIA HIFLD	The locations of ethanol plants with site and company names.
Railroads	HIFLD	Location of railroad tracks by operator.