



STATE ENERGY SECURITY PLAN GUIDANCE

The energy sector is uniquely critical as all other critical infrastructure sectors depend on power and/or fuel to operate. An impact on critical energy infrastructure can directly affect the security and resilience within and across other critical infrastructure sectors – threatening public safety, the economy, and national security.

Energy Security Planning ensures a **reliable** and **resilient** supply of energy through efforts to **identify, assess, and mitigate risks** to energy infrastructure and to **plan for, respond to and recover** from events that disrupt energy supply. Our nation's energy infrastructure and delivery systems are vulnerable to a variety of threats and hazards, including severe weather (exacerbated by climate change), cyberattacks, system failures, pandemics, and deliberate physical attacks. Because most of the nation's critical infrastructure is owned and operated by private companies, both the government and private sector have a mutual incentive to reduce the risk of disruptions to critical infrastructure. It is the responsibility of state and local officials to work with energy providers, across government agencies and with relevant stakeholders to reduce the risk, vulnerabilities, and consequences of an energy disruption or emergency and provide for rapid recovery.

State energy security plans (SESP) are an essential part of energy security planning. SESP describe the state's energy landscape, people, processes, and the state's strategy to build energy resilience. More specifically, the plans detail how a state, working with energy partners, can secure their energy infrastructure against all physical and cybersecurity threats; mitigate the risk of energy supply disruptions to the State; enhance the response to, and recovery from, energy disruptions; and ensure that the state has secure, reliable, and resilient energy infrastructure.

The purpose of this guidance is to provide clarity and detail on the six elements outlined in Section 40108 of the bipartisan *Infrastructure Investment and Jobs Act* (IIJA) hereafter referred to as the "BIL." The U.S. Department of Energy's (DOE) goal is to support states and provide additional clarification beyond the text of the BIL.

The guidance below is the DOE's interpretation of how the six elements could be met – it is not exhaustive. Other methods for meeting the six elements are also acceptable. The example plan layout below provides a logical flow of information, organizing the six elements into practical sections that reduce redundancies. DOE understands that states are working from existing energy security plans and that each of those plans is different. DOE anticipates that states will use different approaches to address the six elements described in the BIL. States do not have to follow this exact format or flow listed below. This is intended to provide examples and to serve as a reference only.

The guidance also references [drop-in resources](#) from the Office of Cybersecurity, Energy Security and Emergency Response (CESER) that will be available in early May 2022. Use of these resources is optional. States can use part or the full "drop-in" and customize for their state needs. These resources are intended to assist states in satisfying the elements outlined in the BIL.



BIL 40108 Provision Excerpt:

FINANCIAL ASSISTANCE FOR STATE ENERGY SECURITY PLANS. —Federal financial assistance made available to a State under this part may be used for the development, implementation, review, and revision of a State energy security plan that—

- 1) assesses the existing circumstances in the State; and
- 2) proposes methods to strengthen the ability of the State, in consultation with owners and operators of energy infrastructure in the State
 - a. to **secure** the energy infrastructure of the State against all physical and cybersecurity threats;
 - b. to **mitigate** the **risk** of energy supply disruptions to the State; and to **enhance the response** to, and **recovery** from, energy disruptions; and
 - c. to ensure that the State has **reliable**, secure, and resilient energy infrastructure.

Contents of Plan. --A State energy security plan shall--

- (1) address all energy sources and regulated and unregulated energy providers;
- (2) provide a State energy profile, including an assessment of energy production, transmission, distribution, and end-use;
- (3) address potential hazards to each energy sector or system, including--
 - physical threats and vulnerabilities; and ``
 - cybersecurity threats and vulnerabilities; ``
- (4) provide a risk assessment of energy infrastructure and cross-sector interdependencies;
- (5) provide a risk mitigation approach to enhance reliability and end-use resilience; and
- (6) address
 - multi-State and regional coordination, planning, and response; and
 - coordination with Indian Tribes with respect to planning and response; and
 - to the extent practicable, encourage mutual assistance in cyber and physical response plans.



STATE ENERGY SECURITY PLAN FRAMEWORK

SECTION	DESCRIPTION	Relative BIL Section (Elements 1-6)
1. Intro / Navigation	<ul style="list-style-type: none"> Describes purpose of each section 	
2. Energy Landscape and Risk Profiles	<p>State Energy Profile: Provide baseline data, maps, and other information on state markets and infrastructure for all energy sources (electricity, liquid fuels, and natural gas), including:</p> <ul style="list-style-type: none"> Production – in-state energy production, including electricity generation by fuel and oil and gas upstream production and refining/processing Transmission - interstate energy transfers and imports, including information on major pipelines, transmission lines, and marine and rail infrastructure Distribution – overview of energy providers in the state, including electric utilities, natural gas local distribution companies, and liquid fuels terminal operators and fuel distributors End-Use- energy demands, including information on seasonal and intraday variability, demands by sector, and any state-specific fuel specifications <p>As appropriate, the profile should include discussion of wider interstate and regional energy markets.</p>	<p>1 address all energy sources and regulated and unregulated energy providers;</p> <p>2 provide a State energy profile, including an assessment of energy production, transmission, distribution, and end-use;</p>
	<p>Threats/Vulnerabilities: Provide information on threats and vulnerabilities to state or regional energy sectors or systems.</p> <ul style="list-style-type: none"> <u>Threat</u> information includes anything that can expose a vulnerability and damage, destroy, or disrupt energy systems, including natural, technological, manmade/physical, and cybersecurity hazards. <u>Vulnerabilities</u> are weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Vulnerabilities may be specific to the threat, energy type, and infrastructure component. <p>Information for this section can be drawn from several sources, including DOE state risk profiles, state hazard mitigation plans, state integrated resource plans, utility emergency plans, and after-action reports for previous incidents, and discussions with energy system operators and other stakeholders.</p>	<p>3 address potential hazards to each energy sector or system, including—</p> <ul style="list-style-type: none"> a. physical threats and vulnerabilities; and b. cybersecurity threats and vulnerabilities;
	<p>Assessing risk to energy infrastructure is a complex, ever evolving, and continuous process with many different stakeholders and systems. Knowing how susceptible an energy asset is to a disruption (natural or man-made) allows decision makers to focus resources on better protecting the most vulnerable assets.</p> <p>Assessment: Conduct risk assessments and analyze cross-sector interdependencies for energy infrastructure assets within the state.</p>	<p>4 provide a risk assessment of energy infrastructure and cross-sector interdependencies;</p>



	<ul style="list-style-type: none"> • Risk Assessment of Energy Infrastructure: Risk is defined as the potential for loss, damage, or destruction of key resources or energy system assets resulting from exposure to a threat. Risk assessments consider the consequence of an asset’s loss, the vulnerability of an asset to specific threats, and the likelihood that an asset will be exposed to a specific threat. Certain energy infrastructure assets may be especially important to ensuring energy infrastructure continuity. Being able to identify the assets that are most critical to the infrastructure or that provide significant support to other critical infrastructure systems helps to determine overall risk and prioritize mitigation strategies more effectively. <i>(Risk assessments may help inform prioritization of 40101 funds)</i> <u>Cross-Sector Interdependencies:</u> consider interdependencies between the energy sector and other sectors and between different energy sub-sectors (electricity, liquid fuels, and natural gas). Understanding the interconnected nature of energy infrastructure and the interdependencies can identify the possible cascading impacts of a disruption. 	
3. Energy Security and Emergency Response Authorities	a) Provide relevant authorities, doctrines, and guiding statutes for energy security and emergency response activities, including federal, state, and local government authorities and emergency response structures.	1 assesses the existing circumstances in the State
4. Energy Security Planning & Preparedness	a) Document State Energy Office roles and responsibilities, which may include monitoring energy markets, mutual assistance work, holding/ participating in staff training & exercises, engaging with stakeholders, updating the energy security plan, completing after-action reports, and undergoing continuous improvement b) Roles of Other State Entities c) Describe Tribal Coordination d) Describe coordination, planning and response activities with neighboring states and the region. Include city and county coordination as appropriate.	6 a) address <ol style="list-style-type: none"> multi-State and regional coordination, planning, and response; and coordination with Indian Tribes with respect to planning and response; encourage mutual assistance in cyber and physical response plans.
5. Energy Emergency Response	Describe response actions /authorities for energy emergencies, including power outages/electricity shortages, liquid fuels shortages, and natural gas shortages. Components may include: <ol style="list-style-type: none"> Response Cycle Overview Information Gathering/Situational Awareness Event Consequence Assessment Response Actions 	6, 2b ... mitigate the risk of energy supply disruptions to the State; and to enhance the response to, and recovery from, energy disruptions;
6. Energy Resiliency & Hazard Mitigation	a) Mitigation approach: provide a strategy for reducing the potential consequences of energy disruptions. The mitigation strategy should describe how energy sector stakeholders will accomplish the goals of strengthening energy sector reliability, enhancing energy supply resilience for end-users, and securing critical energy infrastructure. The approach to prioritize funding and implementation should leverage a risk assessment if feasible. Specific projects and activities can be mentioned. b) <i>Link to 40101 (optional)</i>	5 provide a risk mitigation approach to enhance reliability and end-use resilience; and other entities responsible for—
7. Appendix		



STATE ENERGY SECURITY PLAN (SESP) DETAILED FRAMEWORK

1) INTRO/NAVIGATION

2) ENERGY & RISK PROFILES (1, 2, 3, 4)

- a) **State Energy Profile:** Overview of energy supply, demand, import/export, and infrastructure. Includes EIA data, maps, and lists of key infrastructure and service providers. For all energy types: Electricity (includes: coal, nuclear, and renewable energy), Natural Gas, and Liquid Fuels (includes: biofuels and propane)
 - i) *CESER instructions: How to develop a profile using EIA Data*
 - ii) *Limited example based on EIA data with appropriate analysis*
- b) **Threats/Vulnerabilities:**
 - i) Threats
 - (1) Data on historic emergency events and energy disruptions
 - (a) CESER State and Regional Risk [Profiles](#)
 - (2) Cybersecurity Threats
 - (a) *Drop-in: Cyber IT / OT overview and 2 graphics*
 - (b) *Drop-In: Conversation guidance to gather state specific information*
 - ii) Vulnerabilities
 - (1) Descriptions of vulnerabilities
 - (a) *Drop-In: CESER developed supply chain graphics for each energy type*
- c) **Risk Assessment:**
 - (1) Cross-Sector Interdependencies:
 - (a) Description of interdependencies
 - (b) *Drop-In: CESER developed 3 diagrams*
 - (2) Risk Assessment of Critical Infrastructure:
 - (a) State Critical Infrastructure Analysis

3) ENERGY SECURITY AND EMERGENCY RESPONSE AUTHORITIES (1)

- a) **Relevant Authorities, Doctrines, and Guiding Statutes**
 - i) Requirements to have SESP and plan to maintain and strengthen
 - ii) Authorities
 - (1) Relevant Federal Authorities & Organization Structure
 - (a) *Drop-In: Federal Authorities*
 - (2) Relevant State Authorities
 - (a) emergency response laws and authorities' relevant to energy resources
 - (b) Other state departments or agencies which deal with interdependent sectors (Air Quality, Transportation, Water/Wastewater, Health, etc.
 - (3) Relevant local and tribal authorities (e.g., home rule)



4) ENERGY SECURITY PLANNING & PREPAREDNESS (6)

a) State Energy Office Roles and Responsibilities

i) State Energy Office Responsibilities

(1) **Monitoring Energy Markets**

- (a) Monitor market and supply data
- (b) Review DOE CESER communications on threats/events

(2) **Assess Mitigation, Impact and Response Actions** (e.g., conservation, regulatory, consumer protection, waivers, supply acquisition, subsidies)

(3) **State Energy Emergency Assurance Coordinators (EEAC) Program**

(a) *Drop-In: EEAC overview*

(4) **Stakeholder Engagement**

- (a) Sustain relationships with public and private energy suppliers and other key stakeholders
- (b) Maintain stakeholder contact lists
 - (i) *Drop-In: Contact list template (part of emergency playbook)*

(5) **Staff Training and Exercises**

(6) **After Action Reporting, Evaluation, and Continuous Improvement**

(7) **State emergency response responsibilities**

- (a) Coordination and Roles
- (b) Public Information Program
- (c) With non-government and private sector entities (NASEO included)
- (d) With other states (Multi-State Coordination)
- (e) With federal government
- (f) Contacts (refer to annex)

b) Roles of Other State Entities Relating to Energy Security

- i) Governor's Office
- ii) Governor's Energy Advisor
- iii) Public Utility Commissions (PUC)
- iv) Emergency Management Agencies (EMA)
- v) Homeland Security Agency (HSA)
- vi) Fusion Center

c) Tribal Coordination

- i) Coordination with Indian Tribes with respect to planning and response;

d) Regional Structures and Coordination

- i) Applicable elements from other states' plans in region
- ii) Regional implementation plans and any agreements/MOUs/plans related to mutual assistance to cyber and physical responses.

5) ENERGY EMERGENCY RESPONSE (6, 2B)

(Drop-In: CESER/NASEO customizable state Energy Emergency Response Playbook)

a) Response Cycle Overview

- i) Information Gathering a Consequence Assessment a Response

b) Information Gathering/Situational Awareness (for each energy type)

- i) Situational Awareness Tools (e.g., DOE tools, EIA tools)
- ii) Weather Threat Monitoring Tools (e.g., NOAA hurricane tracks, blizzard forecasts)
- iii) Industry, Peer, and Regional Outreach

c) Consequence Assessment Guidelines (for each energy type)

- i) Guidance on Event Classification/Ratings: Tiers of event consequences



ii) Event Assessment Factors:

- (1) Threat Information (identify threats to energy infrastructure)
- (2) Impacts to energy consumers
- (3) Impacts to critical energy delivery systems (e.g., critical power plants)
- (4) Impacts to bulk/ wholesale energy markets (e.g., bulk fuel stocks)

d) **Response Actions**

i) Response Action Matrices

- (1) Event Type (Power Outage, Natural Gas Shortage, Liquid Fuels Shortage, Multi-System Failure)
 - (a) Event consequence tiers and event stage (pre-event, response/restoration)

6) ENERGY RESILIENCY & HAZARD MITIGATION (5)

a) **State approach** (prioritization, grants, public-private partnerships)

- i) *Drop-In: CESER developed a simple list of general mitigation measures (e.g., system segmentation, smart grids, backup generation at gas stations) as well as measures by hazard type. (e.g., raising substations in flood prone areas)*

7) APPENDICIES

a) **Appendix: SESP Connection to Relevant State Plans**

- i) Long term State Energy Plans
- ii) Hazard Mitigation Plans
- iii) Climate Adaptation Plans
- iv) Resilience Plans
- v) Critical Infrastructure Protection Plans
- vi) State COOP plans
- vii) Utility Integrated Resource Plans
- viii) Citizen Service Programs (LIHEAP, WAP, assistance programs, etc.)
- ix) Others

b) **Other Relevant Energy Sector Risk Assessments/Resources**

- i) NIPP, THIRA – energy integration, Cybersecurity Risk Assessments

c) **Appendix: Data/Situational Tools** (*Drop-in: included in emergency playbook*)

- i) EAGLE-I
- ii) ISO System Condition Pages
- iii) EIA: Grid Monitor, Weekly Petroleum Status Report, Heating Fuels and Energy Atlas
- iv) Natural Gas Pipeline Online Bulletin Boards