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 to 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. SESPs 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 specific language of the elements is provided on the next page of this guidance.

The guidance below is the U.S. Department of Energy's (DOE) interpretation of how the six elements could be met – it is not exhaustive. Other methods for meeting the six elements are also acceptable. 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 resources available online from the Office of Cybersecurity, Energy Security and Emergency Response (CESER). Use of these resources is optional.

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: CONTENTS OF PLAN

SECTION	DESCRIPTION	Relative BIL Section (Elements 1-6)
1. Introduction / Navigation	• Describes purpose of each section and the plan, may include an executive summary.	
2. State Energy Profile	**State Energy Profile:** Provide baseline data, maps, and other information describing state markets and infrastructure for all energy sources (electricity, liquid fuels, and natural gas), including: • **Production** – list in-state energy production sources and providers, including electricity generation by fuel and oil and gas upstream production and refining/processing • **Transmission** – describe interstate energy transfers and imports, including information on major pipelines, transmission lines, and marine and rail infrastructure • **Distribution** – provide an 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**- provide statistical information on energy demand over time by sector (residential, commercial, industrial, transportation), including information on seasonal and intraday variability, trends and forecasts and any state-specific fuel specifications As appropriate, the profile should include discussion of interstate and regional energy markets.	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; 1 assess the existing circumstances in the State
3. Risk Components: Hazards, Threats, Vulnerabilities and Consequences	Provide information on hazards, threats, vulnerabilities, and consequences to state critical energy infrastructure. • A "threat" refers to anything that can damage, destroy, or disrupt energy systems, including natural, technological, human/physical, and cybersecurity threats. • "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, process, or the degree of susceptibility to various threats. 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. • "Consequence" refers to the effect of the loss or degradation of an energy infrastructure system or asset, including the immediate "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. The "indirect consequence" refers to the cost to society of the loss in energy supply, which may include economic losses, loss of life or human health, loss	3 address potential hazards to each energy sector or system, including— a. physical threats and vulnerabilities; and b. cybersecurity threats and vulnerabilities;

	of dependent infrastructure functionality, loss of customer service, and degradation of public opinion and trust. 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. 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.	
4. Risk Assessment of Critical Energy Infrastructure and Interdependencies	Conduct a risk assessment and analyze cross-sector interdependencies for critical energy infrastructure assets within the state. Risk Assessment of Energy Infrastructure: Risk is defined as the potential for loss, damage, or degradation of energy supply or services, and the associated secondary impacts of those losses on society, resulting from the exposure of energy infrastructure to a threat. Each risk is specific to a "Risk Scenario"—a hypothetical situation comprised 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. Risk Assessments may help inform prioritization of Risk Mitigation efforts, including the prioritization of investments made with 40101d funds for Grid Resilience and Reliability Critical Energy Infrastructure: Critical infrastructure assets within the state can be identified through a review of regional energy systems and markets within three key areas: electricity, petroleum, and natural gas. Assets within these systems are identified as critical if their loss would have a major impact on the state's energy supply and/or on the overall reliability of the energy system. 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. Cross-Sector Interdependencies: 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.	4 provide a risk assessment of energy infrastructure and cross-sector interdependencies;

5. Energy Risk Mitigation Approach	Mitigation approach: provide a strategy for responding to priority energy risks identified in the risk assessment. Specific programs, policies, plans, projects and activities can be mentioned as mitigation (such as any funded via 40101d). The approach should prioritize mitigation actions and describe how implementation of mitigation measures will enhance energy system reliability and end-use resilience.	5 provide a risk mitigation approach to enhance reliability and end-use resilience; and other entities responsible for— a. maintaining fuel or electric reliability; and securing energy infrastructure.
6. Energy Security Coordination/ Energy Emergency Response	• 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 • Roles of Other State Entities • Describe Tribes in the state and energy security/emergency response, planning, and coordination activities with the Tribes • Describe coordination, planning and response activities with neighboring states and the region. Include local, city and county coordination as appropriate. Island territories and states outside of the continental U.S. will have a different approach to regional coordination than states in the CONUS. • Authorities: 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. • Emergency Response Protocols: Describe response actions /authorities for energy emergencies, including power outages/electricity shortages, liquid fuels shortages, and natural gas shortages. Components may include: • Response Cycle Overview • Information Gathering/Situational Awareness • Event Consequence Assessment • Response Actions and/or state ESF-12 plan	6, 2b address i. multi-State and regional coordination, planning, and response; and ii. coordination with Indian Tribes with respect to planning and response; iii. encourage mutual assistance in cyber and physical response plans. mitigate the risk of energy supply disruptions to the State; and to enhance the response to, and recovery from, energy disruptions
7. Appendix		

STATE ENERGY SECURITY PLAN (SESP) DETAILED FRAMEWORK

1) INTRODUCTION/NAVIGATION

2) STATE ENERGY PROFILE

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*

3) HAZARDS, THREATS, VULNERABILITIES AND CONSEQUENCES

a) Hazards/Threats

(1) Inventory of hazards and threats that cause energy disruptions

(a) Extract relevant components of the CESER State and Regional Risk Profiles

(b) Historic data as well as trends and forecasts about hazards and threats into the future

(2) Cybersecurity Threats

(a) *Drop-in: Cyber IT / OT overview and 2 graphics*

(b) *Drop-In: Conversation guidance to gather state specific information*

(c) *Reference state Fusion Center information and other state authorities (even those that fall outside of the office completing the plan)*

b) Vulnerabilities

(1) Descriptions of vulnerabilities

(a) *Drop-In: CESER developed supply chain graphics for each energy type, to be used with additional context related to state-specific considerations*

4) RISK ASSESSMENT OF CRITICAL ENERGY INFRASTRUCTURE AND INTERDEPENDENCIES

a) Risk Assessment of Critical Energy Infrastructure

b) Cross-Sector Interdependencies:

(a) Description of interdependencies, with state-specific information

(b) *Drop-In: CESER developed three diagrams*

5) ENERGY RISK MITIGATION APPROACH

a) State approach to responding to priority energy risks

(1) Describe strategies for mitigation, such as public-private partnerships

(2) Describe existing relevant mitigation measures, such as an incentive program

(3) Describe potential mitigation measures and their sources, such as other state plans

(4) Indicate method for prioritization

(5) *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)* *States are encouraged to whittle the list down to just those measures that are realistically able to be deployed*

(due to policy and other constraints, every measure may not be applicable to your state).

6) ENERGY SECURITY COORDINATION

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, Regional, National Coordination**
         (a) Drop-In: EEAC overview should be supplemented with other state and region specific activities
      (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) Description of federally-recognized Tribes, if not a part of the Energy Profile
   ii) Energy security coordination activities with Tribes

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.

e) **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)

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

i) Response Cycle Overview
(1) Information Gathering a Consequence Assessment a Response
ii) Information Gathering/Situational Awareness (for each energy type)
(1) Situational Awareness Tools (e.g., DOE tools, EIA tools)
(2) Weather Threat Monitoring Tools (e.g., NOAA hurricane tracks, blizzard forecasts)
(3) Industry, Peer, and Regional Outreach
iii) Consequence Assessment Guidelines (for each energy type)
(1) Guidance on Event Classification/Ratings: Tiers of event consequences
(2) Event Assessment Factors:
(a) Threat Information (identify threats to energy infrastructure)
(b) Impacts to energy consumers
(c) Impacts to critical energy delivery systems (e.g., critical power plants)
(d) Impacts to bulk/ wholesale energy markets (e.g., bulk fuel stocks)
iv) Response Actions
(1) Response Action Matrices
(a) Event Type (Power Outage, Natural Gas Shortage, Liquid Fuels Shortage, Multi-System Failure)
(i) Event consequence tiers and event stage (pre-event, response/restoration)

7) APPENDICES

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