Energy

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)

May 2007

Homeland Security

Department of Energy

Department of Energy

Washington, DC 20585

FROM: Kevin Kolevar, Director
Office of Electricity Delivery and Energy Reliability

SUBJECT: Release of the Sector Specific Plan

In its role as the Sector Specific Agency (Energy), the Department of Energy has worked closely with the Department of Homeland Security and dozens of government and industry security partners to prepare this 2006 Energy Sector Specific Plan (SSP). Much of that work was conducted through the Energy Sector Coordinating Councils (SCC) and through the Energy Government Coordinating Council (GCC). The Electricity SCC represents over 95 percent of the electric industry and the oil and natural gas SCC represents over 98 percent of its industry. The Government Energy Coordinating Council represents all levels of government – Federal, state, local, and tribal – that are concerned with the energy sector.

We have received considerable support from our sector security partners in this effort. The development process included eight joint writing teams, two formal rounds of reviews and consideration of over 700 comments.

Protecting and improving the resiliency of the energy sector in the face of both man-made and natural disasters will be an ongoing effort that will require continued vigilance, contingency planning, and training. The sector security vision and goals communicate the physical and cyber preparedness, protective, and recovery measures that the government and infrastructure owners and operators are working together to achieve.

Perhaps the most valuable aspect of the SSP development process has been the establishment of even more open communication and the ongoing development of a trusted relationship and true partnership between government and industry. This partnership has enabled the development of a unified vision for the energy sector, and it will continue to facilitate the national effort to implement the energy sector's CI/KR protective programs.

We look forward to working with our sector partners in the implementation of the plan in our efforts to improve the reliability and resilience of the energy sector.

Sincerely,

Kevin M. Kolevar
Director, Office of Electricity Delivery and Energy Reliability, U.S Department of Energy

Energy Sector Coordinating Councils Letter of Concurrence

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of federal critical infrastructures and key resources (CI/KR) protection efforts into a single national program. The NIPP includes an overall framework integrating federal programs and activities that are currently underway in the various sectors, as well as new and developing CI/KR protection efforts. The Energy Sector-Specific Plan (SSP) details the application of the NIPP's overall risk management framework to the Energy Sector.

The Energy SSP describes a collaborative process between the private sector, state, local, and tribal governments, nongovernmental organizations, and the Federal Government. This collaboration is intended to help DOE in the prioritization of its protection and preparedness initiatives and investments within and across sectors. This prioritization is intended to help ensure that government resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, minimizing the consequences of attacks and other incidences, and enhancing recovery.

The members of the Energy Sector Coordinating Councils acknowledge that they:

- Will continue to work with the U.S. Department of Energy and the related Government Coordinating Council on the issues and processes identified in the SSP;
- Have had the opportunity to provide insights and guidance on the unique needs, concerns, and perspectives of their organizations or members;
- Will maintain partnerships for CI/KR protection with appropriate Federal, State, regional, local, tribal, and international entities; other private sector entities; and nongovernmental organizations; and
- Will work with DHS and the U.S. Department of Energy to find mutually acceptable mechanisms to protect and share CI/KR information.

Kevin Kolevar
Chairman
Government Coordinating
Council

Stuart Brindley
Chairman
Electricity Sector
Coordinating Council

Gary Forman
Chairman
Oil and Natural Gas
Coordinating Council

Table of Contents

Executive Summary 1

Energy Sector Profile and Assets 2

CI/KR Assessment and Prioritization 3

Protective Programs and Performance Measurement 3

CI/KR Protection R&D 3

Energy SSP Process and Responsibilities 4

Introduction 5

1. Sector Profile, Vision, and Goals 7

1.1 Sector Security Vision and Goals 8

1.1.1 Vision Statement 8

1.1.2 Goals 8

1.2 Sector Profile 8

1.2.1 Electricity 9

1.2.2 Petroleum 12

1.2.3 Natural Gas 15

1.2.4 Energy Sector Interdependencies 17

1.3 Security Partners 18

1.3.1 Relationships With Industry Owner/Operators and Organizations 18

1.3.2 Relationships With Government Agencies 18

1.4 Value Proposition 21

2. Identify Assets, Systems, Networks, and Functions 23

2.1 Defining Information Parameters 23

2.1.1 Energy Assets and Systems 23

2.1.2 Defining Energy Asset and System Parameters 25

2.1.3 Information Collection and Sharing 25

2.1.4 Existing Energy Sector Information Resources 26

2.2 Collecting Infrastructure Information 27

2.3 Verifying and Updating Infrastructure Information 27

3. Assess Risks 29

3.1 Use of Risk Assessment in the Sector 30

3.2 Screening Infrastructure 31
3.3 Assessing Consequences 31
3.4 Assessing Threats 32
3.5 Assessing Vulnerabilities 33
4. Prioritize Infrastructure 35
5. Develop and Implement Protective Programs 37
5.1 Overview of Sector Protective Programs 37
5.2 Process for Evaluating, Prioritizing Needs, and Implementing Programs 37
5.2.1 Enhanced Information Sharing and Needs Assessment 38
5.2.2 Developing and Implementing Focused Programs 39
5.3 Program Development and Sector Goals 39
5.3.1 Information Sharing and Communication 39
5.3.2 Physical and Cyber Security 41
5.3.3 Coordination and Planning 43
5.3.4 Public Confidence 46
5.4 Program Performance, Gaps, and Challenges 47
6. Measure Progress 49
6.1 CI/KR Performance Measurement 50
6.1.1 Metrics 50
6.1.2 Information Collection and Verification 50
6.1.3 Reporting 50
6.2 Implementation Actions 50
6.3 Challenges and Continuous Improvement 51
7. CI/KR Protection R&D 53
7.1 Strategies for Securing Control Systems in the Energy Sector 53
7.2 Energy Sector R&D Requirements 54
7.3 Sector R&D Plan 57
7.4 R&D Management Processes 57
8. Managing and Coordinating SSA Responsibilities 59
8.1 Program Management Approach 59
8.2 Processes and Responsibilities 59
8.2.1 SSP Maintenance and Update 59
8.2.2 Annual Reporting 59
8.2.3 Resources and Budgets 60
8.2.4 Training and Education 60
8.3 Information Sharing and Protection 60

Appendix 1: List of Acronyms and Abbreviations 61
Appendix 2: Sources and References 63
Appendix 3: Authorities 67
Appendix 4: Asset Ownership 77
Appendix 5: Energy SCC and GCC Membership and Participation 79
Appendix 6: Transportation SSP: Pipeline Modal Implementation Plan Executive Summary 83
Appendix 7: Select Energy-Related Cyber R&D Programs 85

List of Figures

Figure I-1. NIPP Risk Management Framework 6
Figure 1-1. Establishing Security Goals 7
Figure 1-2. Overview of the Electric Power System and Control Communications 10
Figure 1-3. 2005 Electricity Statistics 11
Figure 1-4. 2005 Petroleum Statistics 12
Figure 1-5. Overview of the Petroleum System 13
Figure 1-6. 2005 Natural Gas Statistics 15
Figure 1-7. Flow of Natural Gas 15
Figure 1-8. Interdependencies Across the Economy 17
Figure 2-1. Identify Assets, Systems, Networks, and Functions 23
Figure 2-2. Reliable Operation of the North American Electric Power Grid System 24
Figure 3-1. Assess Risks 29
Figure 4-1. Prioritize 35
Figure 5-1. Implement Protective Programs 37
Figure 5-2. Evaluating and Prioritizing Needs, and Implementing Programs 38
Figure 5-3. ESISAC Functions 40
Figure 5-4. Oil and Natural Gas Homeland Security Information Network Functions 41
Figure 5-5. Public Utility Commissions 45
Figure 5-6. Southeastern Electric Exchange Mutual Assistance Group 46
Figure 6-1. Measure Effectiveness 49

List of Tables

Table 1.1. Segments of the Energy Sector 9
Table 1.2. Oil Import Dependence, 2005 14
Table 1.3. Natural Gas Import Dependence, 2005 16
Table 5.1. Energy Sector Gaps and Recommendations 47
Table 7.1. Strategies for Securing Control Systems in the Energy Sector 55
Table A5-1. Organizational Membership on Energy SCC and GCC Membership and Participation 79
Table A7-1. Selection of Cyber Security R&D Programs and Initiatives 86

Executive Summary

In June 2006, the U.S. Department of Homeland Security (DHS) announced completion of the National Infrastructure Protection Plan (NIPP) Base Plan, a comprehensive risk management framework that defines critical infrastructure protection (CIP) roles and responsibilities for all levels of government, private industry, and other security partners. The U.S. Department of Energy (DOE) has been designated the Sector-Specific Agency (SSA) for the Energy Sector,[1] and is tasked with coordinating preparation of an Energy Sector-Specific Plan (SSP) that will be an annex to DHS's NIPP.

In its role as Energy SSA, DOE has worked closely with dozens of government and industry security partners to prepare this 2007 Energy SSP. Much of that work was conducted through the Sector Coordinating Councils (SCC) for electricity and for oil and natural gas, as well as through the Energy Government Coordinating Council (GCC). The electricity SCC represents more than 95 percent of the electric industry and the oil and natural gas SCC represents more than 98 percent of its industry. The GCC, co—chaired by DHS and DOE, represents all levels of government—Federal, State, local, and tribal-that are concerned with the Energy Sector.

The Energy Sector has developed a vision statement and six sector security goals that will be used as the framework for developing and implementing effective protective measures.

Vision Statement for the Energy Sector

The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.

[1] The Energy Sector, as delineated by Homeland Security Presidential Directive 7, includes the production, refining, storage, and distribution of oil, gas, and electric power, except for hydroelectric and commercial nuclear power facilities. This SSP distinguishes between the electricity subsector and the oil and natural gas subsector, although for ease of reading, the terms "subsector" and "sector" are used interchangeably when referring to these two energy sector segments.

Sector Security Goals Information Sharing and Communication
Goal 1: Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector security partners.
Physical and Cyber Security
Goal 2: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.
Coordination and Planning
Goal 3: Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.
Goal 4: Clearly define critical infrastructure protection roles and responsibilities among all Federal, State, local, and private sector security partners.
Goal 5: Understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations.
Public Confidence
Goal 6: Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts.

Energy Sector Profile and Assets

The Energy Sector consists of thousands of electricity, oil, and natural gas assets that are geographically dispersed and connected by systems and networks. Therefore, interdependency within the sector and across the Nation's critical infrastructure sectors is critical. The energy infrastructure provides fuel to the Nation, and in turn depends on the Nation's transportation, communications, finance, and government infrastructures. The energy systems and networks cross the Nation's borders, making international collaboration a necessary component of the Energy Sector's efforts.

Protecting and improving the resiliency of the Energy Sector in the face of both manmade and natural disasters will be an ongoing effort that will require continued vigilance, contingency planning, and training. The sector security vision and goals communicate the comprehensive physical and cyber preparedness, protective, and recovery measures that the government and infrastructure owners and operators are working together to achieve for the sector.

The Energy Sector already has substantial information sources in place to support Critical Infrastructure and Key Resources (CI/KR)[2] protection, planning, and analysis. Collected by owners and operators, trade associations, and government organizations, this information identifies energy assets, systems, and networks. Any critical information that is voluntarily provided to DHS or DOE is expected to be protected by the Protected Critical Infrastructure Information (PCII) Program per the Critical Infrastructure Information Act of 2002 (CII Act). The CII Act provides that information submitted under the PCII Program is protected from

[2] CI/KR can be defined as the assets, systems, networks, and functions that provide vital services to the United States.

public disclosure. In addition to the PCII Program, established communication channels among the sector security partners will enable such critical information to be shared whenever necessary to facilitate protection and recovery of CI/KR.

CI/KR Assessment and Prioritization

Historically, the Energy Sector has been proactive in developing and applying vulnerability assessment methodologies, although no single methodology is universally applicable. Because of the diversity of assets and systems in the Energy Sector, a multitude of methodologies are used to assess risks, vulnerabilities, and consequences. The Energy Sector's threat analysis encompasses natural events, criminal acts, and insider threats, as well as foreign and domestic terrorism. Currently, a number of tools are being used to assess vulnerabilities, and the vast majority of significant facilities have already undergone assessments using one or more of the tools.

As the Energy Sector is characterized by very diverse assets and systems, prioritization of sector assets and systems is highly dependent upon changing threats and consequences. The significance of many individual components in the network is highly variable, depending on location, time of day, day of the week, and season of the year. Owners and operators of the Energy Sector have well-developed protocols in place to identify priorities and ensure business continuity and operational reliability. Therefore, prioritization of assets and systems in the Energy Sector needs to be flexible according to circumstances. Further dialogue with DHS and other stakeholders is necessary to examine cross-sector needs and approaches to support DHS programs.

Protective Programs and Performance Measurement

With partnership as the cornerstone of its overall strategy, the Energy Sector already has numerous programs sponsored by dozens of public and private organizations that support the sector's security vision and goals. The programs fall within four main categories: information sharing and communication, physical and cyber security, coordination and planning, and public confidence. The Energy Sector will continue to implement effective protective measures as it assesses the sector's security needs, develops programs, and finds long-term solutions, including research and development (R&D).

The Energy Sector is in the process of developing an effective performance measurement system that identifies appropriate metrics for measuring progress, collects relevant data on each metric, and uses those data to improve performance and provide accountability. Security metrics are divided into two classes: (1) core metrics established by DHS to be used across all sectors, and (2) sector-specific metrics. Energy sector-specific metrics will be developed by the security partners. In addition, qualitative and quantitative measures to track progress toward the sector goals are currently being developed and will be periodically reviewed and modified as necessary. The Energy Sector has established action items, most of which are already underway, and they will continue to be executed in coordination with all energy security partners.

CI/KR Protection R&D

Energy asset owners and operators have been working with government, national laboratories, universities, industry organizations, and other key stakeholders to drive technological innovation throughout the Energy Sector, including infrastructure and cyber security. The 2006 Roadmap to Secure Control Systems in the Energy Sector established four main security goals and addresses the spectrum of cyber security priorities within the sector. The four goals are: measure and assess security posture; develop and integrate protective measures; detect intrusion and implement response strategies; and sustain security improvements. As improved infrastructure security and resiliency have become an increasingly significant objective of the Energy Sector's technology R&D, Federal R&D investments must be coordinated with the private sector to create an effective national R&D strategy for CIP.

Energy SSP Process and Responsibilities

DOE's Office of Electricity Delivery and Energy Reliability (OE) has taken the responsibility of the Energy SSA and will oversee all activities associated with the NIPP and Energy SSP. In doing so, DOE will maintain a close partnership with the electricity and the oil and natural gas SCCs and governmental partners through the Critical Infrastructure Protection Advisory Council (CIPAC). The Energy SSP will be updated on a regular basis, no less than biennially, for the initial 4 years. After that 4-year period, the SSP will be updated as the NIPP Base Plan is updated. In addition to the Energy SSP, DOE and its security partners will submit an annual CI/KR report to DHS.

Perhaps the most valuable aspect of the SSP development process has been the establishment of even more open communication and the ongoing development of a trusted relationship and true partnership between government and industry. This partnership has enabled development of a unified vision for the Energy Sector, and it will continue to facilitate the national effort to implement the Energy Sector's CI/KR protective programs.

Introduction

On June 30, 2006, the U.S. Department of Homeland Security (DHS) announced completion of the National Infrastructure Protection Plan (NIPP) Base Plan, a comprehensive risk management framework that defines critical infrastructure protection (CIP) roles and responsibilities for all levels of government, private industry, and other security partners. The NIPP builds on the principles of the President's National Strategy for Homeland Security[3] and strategies for the protection of critical infrastructure and key resources (CI/KR).

The NIPP fulfills the requirements of the Homeland Security Act of 2002 that assigns DHS the responsibility to develop a comprehensive national plan for securing CI/KR, as well as Homeland Security Presidential Directive 7 (HSPD-7), which provides overall guidance for developing and implementing the national CIP program. Per HSPD-7, the national infrastructure is divided into 17 distinct CI/KR sectors, and CI/KR protection responsibilities are assigned to select Federal agencies called Sector-Specific Agencies (SSAs). Each SSA is required to complete a Sector-Specific Plan (SSP) for its sector within 180 days of the NIPP's issuance.

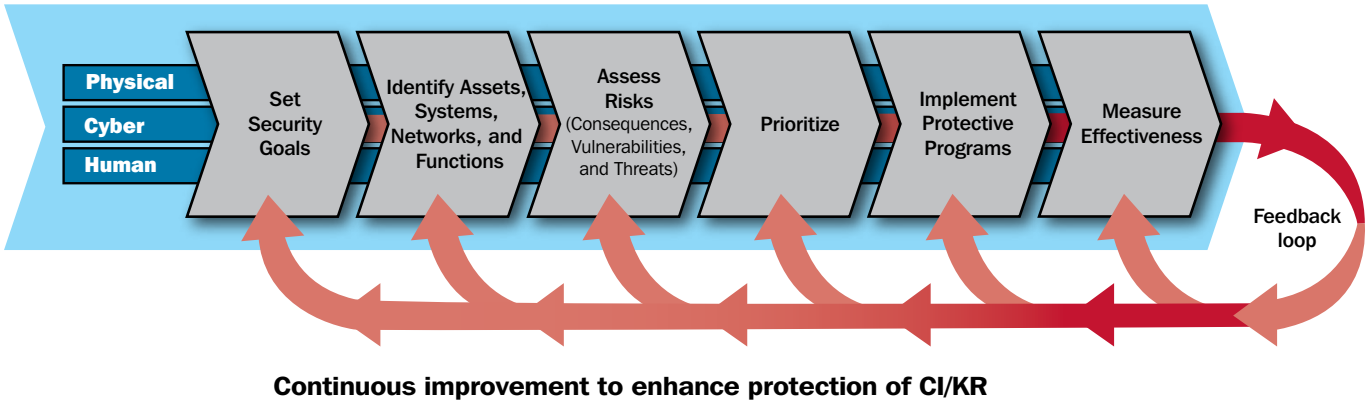
The U.S. Department of Energy (DOE) has been designated the Energy SSA and in this role has closely collaborated with dozens of government and industry security partners to write, review, and revise the 2006 Energy SSP. DOE also conducted two formal review and comment periods for the draft Energy SSP.

The Energy Sector has made significant progress in developing plans to protect the energy CI/KR and to prepare for restoration and recovery in response to terrorist attacks or natural disasters. Through the Energy SSP process, the government and industry have established unprecedented cooperation and a close partnership to develop and implement a national effort that brings together all levels of government, industry, and international partners.

[3] The National Strategy for Homeland Security is the first national strategy established in the aftermath of the September 11, 2001 attacks. Released in July 2002, it is a comprehensive plan for using America's talents and resources to enhance CI/KR protection and reduce vulnerability to terrorist attacks.

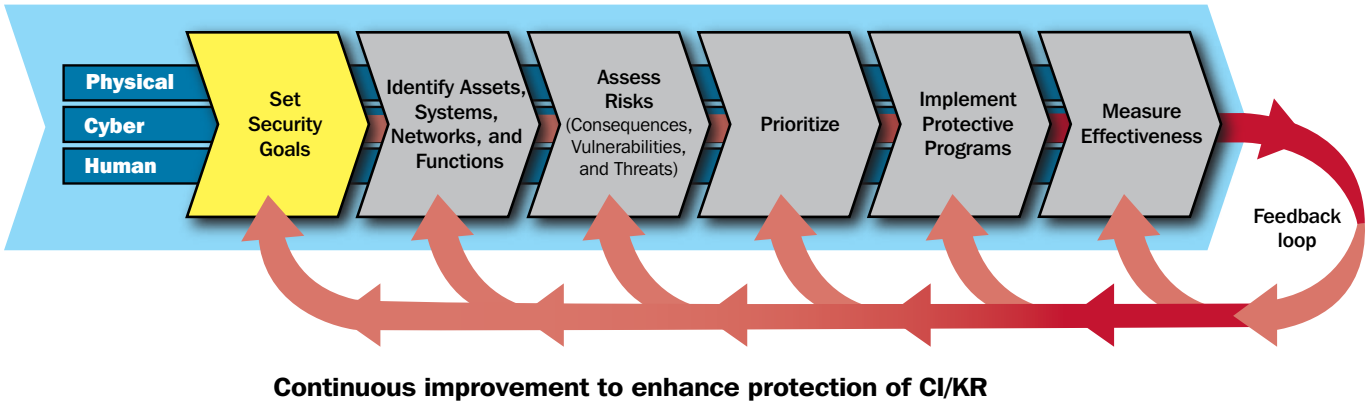
The Energy SSP is structured around the Risk Management Framework defined in the NIPP:

Figure I-1: NIPP Risk Management Framework



1. Sector Profile, Vision, and Goals

Figure 1-1: Establishing Security Goals



A healthy energy infrastructure is one of the defining characteristics of a modern global economy. Any prolonged interruption of the supply of basic energy—electricity, petroleum, or natural gas—would do considerable harm to the U.S. economy and the American people.

Numerous characteristics of the Nation's energy infrastructure, including the wide diversity of owners and operators and the variety of energy supply alternatives and delivery mechanisms, make protecting it a challenge. Energy infrastructure assets and systems are geographically dispersed. There are thousands of miles of electricity lines and oil and natural gas pipelines and many other assets in all 50 States and Territories. In many cases these assets and systems are interdependent. In addition, the Energy Sector is subject to regulation in various forms.

DOE will work with its Energy Sector security partners to improve awareness and information sharing, implement measures to protect and enhance the resiliency of physical and cyber assets, conduct emergency planning, define roles and responsibilities, understand and address interdependencies, and maintain public confidence. This chapter describes the security goals of the Energy Sector, the key characteristics of the electricity, petroleum, and natural gas industries, and the extensive public/private partnership involved in identifying security risks and protecting the energy infrastructure. Appendix 3 provides a brief summary of Federal legislative authorities related to the Energy Sector, and appendix 4 shows types of major asset ownership.

1.1 Sector Security Vision and Goals

Sector security vision and goals communicate the comprehensive preparedness, protective, and recovery measures that the government and infrastructure owners and operators are working together to achieve. They are intended to reflect the sector's overall risk management focus and strategy, and guide the activities of the NIPP Risk Management Framework.

The Energy Sector used a collaborative process to develop its vision statement and security goals. In its role as the designated SSA for energy, DOE worked collaboratively with two energy Sector Coordinating Councils (SCCs)—one for electricity and one for oil and natural gas—and a Government Coordinating Council (GCC) composed of members from all levels of government concerned with maintaining energy security. These coordinating councils represent nearly all members of the energy community and are committed not only to working closely with DOE and other government Energy Sector partners to develop and refine the vision and goals for the sector, but also to working together toward achieving them.

1.1.1 Vision Statement

The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.

1.1.2 Goals

Information Sharing and Communication

- **Goal 1:** Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector security partners.

Physical and Cyber Security

- **Goal 2:** Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.

Coordination and Planning

- **Goal 3:** Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.
- **Goal 4:** Clearly define CIP roles and responsibilities among all Federal, State, local, and private sector security partners.
- **Goal 5:** Understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations.

Public Confidence

- **Goal 6:** Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts.

1.2 Sector Profile

The Energy Sector includes assets related to three key energy resources: electric power, petroleum, and natural gas. Each of these resources requires a unique set of supporting activities and assets, as shown in table 1.1. Petroleum and natural gas share similarities in methods of extraction, fuel cycles, and transport, but the facilities and commodities are separately regulated and have multiple stakeholders and trade associations.

Energy assets and critical infrastructure components are owned by private, Federal, State, and local entities, as well as by some types of energy consumers, such as large industries and financial institutions (often for backup power purposes). Types of major asset ownership are shown in appendix 4.

Table 1.1: Segments of the Energy Sector

Electricity	Petroleum	Natural Gas
• Generation	• Crude Oil	• Production
– Fossil fuel power plants	– Onshore fields	– Onshore fields
Coal	– Offshore fields	– Offshore fields
Gas	– Terminals	• Processing
Oil	– Transport (pipelines)*	• Transport (pipelines)*
– Nuclear power plants*	– Storage	• Distribution (pipelines)*
– Hydroelectric dams*	• Petroleum Processing Facilities	• Storage
– Renewable energy	– Refineries	• Liquefied Natural Gas Facilities
• Transmission	– Terminals	• Control Systems
– Substations	– Transport (pipelines)*	• Gas Markets
– Lines	– Storage	
– Control centers	– Control Systems	
• Distribution	– Petroleum Markets	
– Substations		
– Lines		
– Control centers		
• Control Systems		
• Electricity Markets		

* Hydroelectric dams, nuclear facilities, rail, and pipeline transportation are covered in other SSPs.

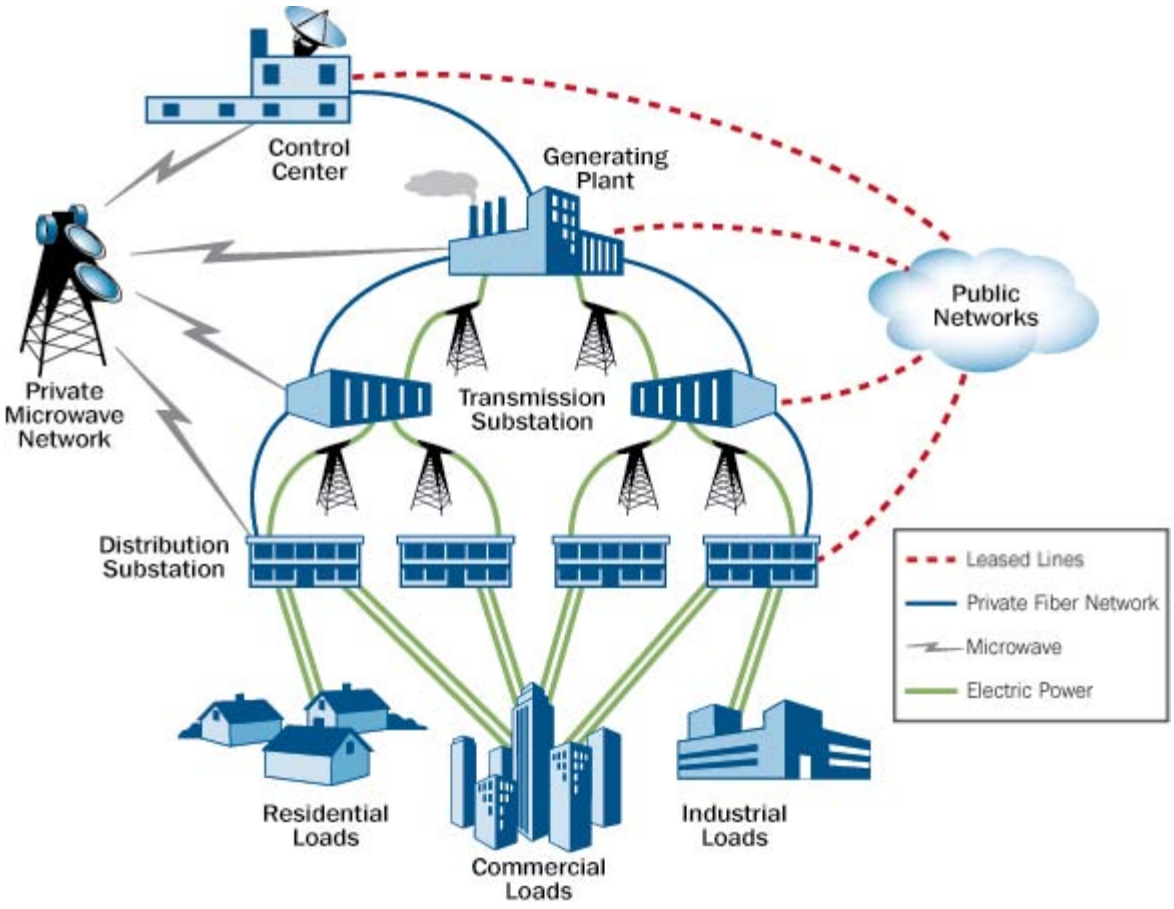
1.2.1 Electricity

The electricity portion of the Energy Sector includes the generation, transmission, and distribution of electricity (figure 1-2). The use of electricity is ubiquitous, spanning all sectors of the U.S. economy. Electric generation accounted for 40 percent of all energy consumed in the United States in 2005.[4] Although there are some significant regional differences, more than 98 percent of electricity is generated domestically, though some of the fuels used to generate electricity are imported.[5]

[4] Energy Information Administration (EIA), *Annual Energy Review* 2005, table 2.1a, www.eia.doe.gov/aer/txt/stb0201a.xls. Coal alone accounts for half of total U.S. generation and, as such, is a key energy source for electricity.

[5] EIA, www.eia.doe.gov/emeu/aer/txt/stb0801.xls.

Figure 1-2: Overview of the Electric Power System and Control Communications



Electricity system facilities are dispersed throughout the North American continent.[6] Although most assets are privately owned, no single organization represents the interests of the entire sector. The North American Electric Reliability Corporation (NERC),[7] through its eight Regional Reliability Councils, provides a platform for ensuring reliable, adequate, and secure supplies of electricity through coordination with many asset owners.

1.2.1.1 Electricity Generation

The burning of fossil fuels (coal, natural gas, and oil) provides more than 70 percent of the electricity generated in the United States, as shown in figure 1-3. Virtually all coal is mined domestically and then transported to power plants by rail and barge. Natural gas and oil are transported to power plants by pipeline.

[6] Important electric systems are also found in Alaska, Hawaii, and the U.S. Territories.

[7] NERC was founded as a nonprofit organization in 1968. It was designated as the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission following passage of the Energy Policy Act of 2005. As a result of the law, NERC's official name changed to the North American Electric Reliability Corporation, effective January 1, 2007. The ERO will develop and enforce mandatory reliability standards for the bulk electric power system in the United States, Canada, and a portion of Baja Mexico.

Several key sources of electricity generation are covered in other sector plans. The nuclear industry is regulated by the Nuclear Regulatory Commission (NRC), an independent Federal agency. Further discussion of nuclear power is provided in the Nuclear Reactors, Materials and Waste SSP developed by NRC in partnership with DHS. In addition, the security of pipelines, which are critical for delivering oil and natural gas to power plants, is covered in the Pipeline Modal Implementation Plan Annex to the Transportation SSP. Discussion of hydropower, including pumped storage, is provided in the Dams SSP developed by DHS in partnership with the United States Army Corps of Engineers (USACE), the Department of the Interior's (DOI) Bureau of Reclamation (BOR), and other public and private dam owners and operators.

Non-hydropower renewable energy sources (e.g., solar, wind, geothermal) account for a small but growing percentage of national electricity generation,[8] with the potential to provide alternative power sources for critical facilities and functions.

1.2.1.2 Electricity Transmission, Distribution, and Control Systems

Transmission lines. Transmission lines serve two primary purposes: They move electricity from generation sites to customers and they interconnect systems. Voltages in the transmission system are high, which makes it possible to carry electric power efficiently over long distances and deliver it to substations near customers.

Figure 1-3: 2005 Electricity Statistics

- 978 gigawatts generating capacity
  - 58 percent utility-owned, 42 percent non-utility
- 6,000 power plants
  - 54 percent utility-owned, 46 percent non-utility
- 4.1 million gigawatt-hours net generation
  - 50 percent coal
  - 19 percent nuclear
  - 19 percent natural gas
  - 7 percent hydro
  - 3 percent oil
  - 3 percent other (solar, wind, geothermal)
- 3,276 utilities
  - 220 investor-owned
  - 884 cooperatives
  - 2,011 publicly owned
  - 152 power marketers
  - 9 Federal power agencies
- 100,000 high-voltage transformers
- 63,000 substations
- 155,000 miles high-voltage AC transmission lines
- 138 million customers

Sources: Generating capacity, power plants, net generation, and customers data from Energy Information Administration; utilities data from American Public Power Association; transformers data from DOE; transmission line data from NERC.

Transmission and distribution substations. Substations are located at the ends of transmission lines. A transmission substation located near a power plant uses large transformers to increase the voltage to higher levels. At the other end of the transmission line, a substation uses transformers to step transmission voltages back down to distribution voltages so the electricity can be distributed to customers.

Control centers. Control centers have sophisticated monitoring and control systems and are staffed by operators 24 hours per day, 365 days per year. These operators are responsible for several key functions, including balancing power generation and demand, monitoring flows over transmission lines to avoid overloading, planning and configuring the system to operate reliably, maintaining system stability, preparing for emergencies, and placing equipment out of service and back into service for maintenance and emergencies.

Distribution lines. Distribution lines carry electricity from substations to end users.

Control systems. Supervisory Control and Data Acquisition Systems (SCADA) and other control systems monitor the flow of electricity from generators through transmission and distribution lines. These electronic systems enable efficient operation and management of electric systems through the use of automated data collection and equipment control.

[8] Data from National Energy Policy, May 2001 (DOE International Emissions Trading Association data).

1.2.2 Petroleum

The petroleum portion of the Energy Sector includes the production, transportation, and storage of crude oil; the processing of crude oil into petroleum products; the transmission, distribution, and storage of petroleum products; and sophisticated control systems to coordinate storage and transportation (figures 1.4 and 1.5).

Petroleum accounted for 40 percent of U.S. energy consumption in 2005. Its primary use is in the Transportation Systems Sector, where it accounts for 98 percent of energy consumption.[9] Petroleum is used to lesser degrees in other sectors, accounting for 30 percent of energy used in the industrial sector, 7 percent in the residential, 4 percent in the commercial, and 3 percent in the electric power sector.[10]

As previously noted, pipelines, which are critical for the gathering, transmission, and distribution of petroleum and natural gas, are part of the transportation sector, and oversight of pipeline security is the responsibility of DHS's Transportation Security Administration (TSA). Pipeline security is specifically addressed in the Pipeline Modal Implementation Plan Annex to the Transportation Systems SSP developed by TSA. The executive summary of the plan is also appended to the Energy SSP as appendix 6.

Figure 1-4: 2005 Petroleum Statistics

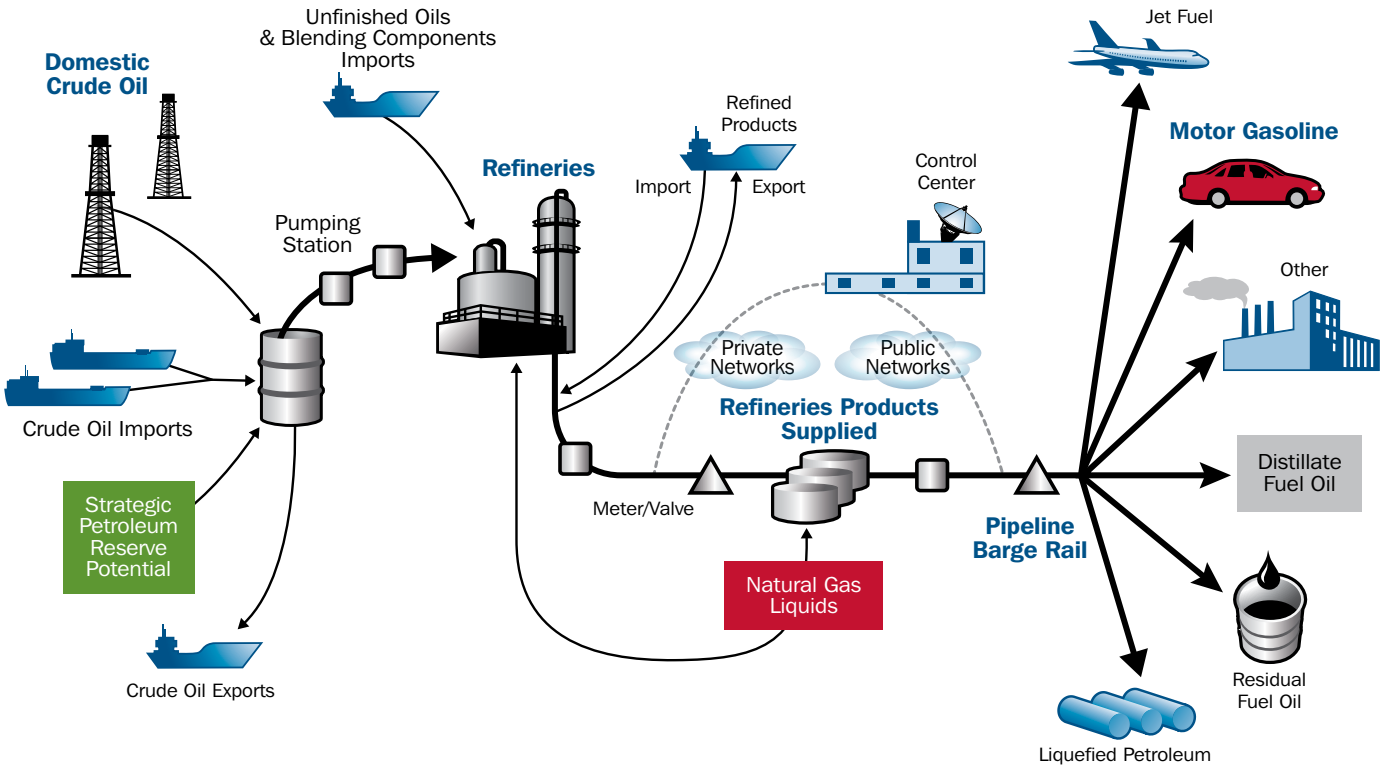
Production	506,000 producing wells
Gathering	>30,000 miles of gathering pipeline
Processing	149 petroleum refineries
Storage	1,400 petroleum terminals
Transportation (2004)	66 percent pipelines
	27 percent water carriers
	4 percent motor carriers
	2 percent railroads
Pipelines (2004)	284 billion ton miles of crude pipelines
	316 billion ton miles of product pipelines

Sources: Production and processing data from EIA; data on terminals from Oil Price Information Service; gathering data from The Steering Committee on Energy Pipe Lines and Research; transportation data from Association of Oil Pipe Lines. Note: Percent share calculated from billion ton miles.

The Energy SSP does not address the chemical industry and the overlap between the petrochemical industry and the transportation, storage, and processing of crude oil and refined petroleum products. Petrochemical facilities are addressed in the Chemical SSP.

[9] EIA, *Annual Energy Review* 2005, table 2.1e, www.eia.doe.gov/emeu/aer/txt/stb0201e.xls.
[10] EIA, *Annual Energy Review* 2005, tables 1.3, 2.1b, 2.1c, 2.1d, 2.1e, and 2.1f, www.eia.doe.gov/emeu/aer.

Figure 1-5: Overview of the Petroleum System



1.2.2.1 Crude Oil

Onshore and offshore fields. U.S. crude oil production is concentrated onshore and offshore along the Texas-Louisiana Gulf Coast, extending inland through west Texas, Oklahoma, and eastern Kansas. There are also significant oil fields in Alaska along the central North Slope. U.S. proved[11] crude oil reserves totaled an estimated 21.8 billion barrels at the close of 2005. More than three-quarters (80 percent) of U.S. reserves are in Alaska, California, Texas, and offshore areas. Petroleum production from the Alaskan North Slope is now equaled by output from the offshore areas in the Federal domain seaward of the coastline along California and the western and central coasts of the Gulf of Mexico.

Crude oil drilling, gathering, and processing. The upstream sector of the petroleum industry includes a large number of facilities, such as wellheads, gas and oil separation plants, oil/gas dehydration units, emulsion breaker units, oil/gas sweetening units, compressor stations, water treatment units, etc., for both onshore and offshore areas.

Import marine terminals. The United States' dependence on foreign crude oil has grown from 15 percent in 1971 to 66 percent in 2005 (table 1.2).[12] Crude oil is received into the United States at import terminals, which usually consist of a berth or port facility for the tankers, unloading facilities, storage facilities, and a system of pipelines to move the crude.

[11] Reserves believed to be recoverable from known reservoirs under existing economic and operating conditions.
[12] EIA, *Annual Energy Review* 2005, tables 5.1, 5.3, and 5.5.

Crude oil transport. Privately owned pipelines transport most of the crude oil in the United States. Waterborne transportation modes, including ocean tankers and barges, are also used.

Crude oil storage. Import terminals always incorporate storage facilities. At the end of 2005, U.S. crude oil inventories, including the Strategic Petroleum Reserve (SPR), totaled 1,008 million barrels.[14] More than two-thirds is stored in huge underground salt caverns at the SPR along the coastline of the Gulf of Mexico. The reserve has the capacity to hold 727 million barrels[15] and is the world's largest supply of emergency crude oil.

Table 1.2: Oil Import Dependence, 2005[13]

U.S. Production	5.1 million barrels/day crude 1.7 million barrels/day natural gas plant liquids
Net Imports	10.1 million barrels/day crude 3.5 million barrels/day petroleum products
Import Dependence	66 percent for crude oil

1.2.2.2 Petroleum Processing, Product Transport, and Storage

Refineries. Refineries process crude oil into petroleum products such as gasoline, diesel fuel, jet fuel, and home heating oil. The Gulf Coast has more than twice the crude oil distillation capacity of any other U.S. region. Over the last 20 years, the number of U.S. oil refineries has declined from 223 in 1985 to 148 in 2005, while total capacity has increased by more than 1.5 million barrels per day (10 percent) to more than 17 million barrels per day. Over the last 5 years, gross inputs to the nation's refineries have been at their highest level in history, at nearly 15.5 million barrels per day-19 percent higher than the 5-year average for 1985-1989.[16] Over the past 5 years, refineries have been operating at roughly 92 percent of capacity, with summer peak utilization rates of approximately 95 to 97 percent.

Petroleum product transport. Petroleum products are mainly transported by pipeline, tanker, or barge, but railroad tank cars or trucks are also used. The products are shipped to terminals for temporary storage before transport to smaller bulk plants in market areas.

Petroleum product storage. Petroleum products are stored both above and below ground in tank farms and storage fields to minimize unwanted fluctuations in pipeline throughput and product delivery. DOE's Northeast Home Heating Oil Reserve stores 2 million barrels of home heating oil at commercial terminals in the Northeast. This oil is intended for distribution during severe heating-oil supply disruptions in that part of the country.

1.2.2.3 Petroleum Control Systems

Control systems continuously monitor, transmit, and process pipeline data (e.g., flow rate, pressure, speed). SCADA systems monitor and control pumping stations and track terminal inventories.

[13] EIA, *Annual Energy Review* 2005, tables 5.1, 5.3, and 5.5.

[14] EIA, *Petroleum Supply Annual* 2005, www.eia.doe.gov/emeu/aer/txt/stb0516.xls. In an energy emergency, SPR oil would be distributed by competitive sale. Decisions to withdraw crude oil from the reserve are made by the President under the authorities of the Energy Policy and Conservation Act (42 U.S.C. 6241(d)(1).

[15] DOE, Office of Fossil Energy, www.fe.doe.gov/programs/reserves/spr/spr-facts.html.

[16] EIA, refinery counts from http://tonto.eia.doe.gov/dnav/pet/hist/8_na_8o0_nus_ca.htm; capacity from http://tonto.eia.doe.gov/dnav/pet/hist/mocleus2a.htm; gross inputs from http://tonto.eia.doe.gov/dnav/pet/hist/mgirius2a.htm.

1.2.3 Natural Gas

The natural gas portion of the Energy Sector includes the production, processing, transportation, distribution, and storage of natural gas; liquefied natural gas (LNG) facilities; and gas control systems (figures 1.6 and 1.7).

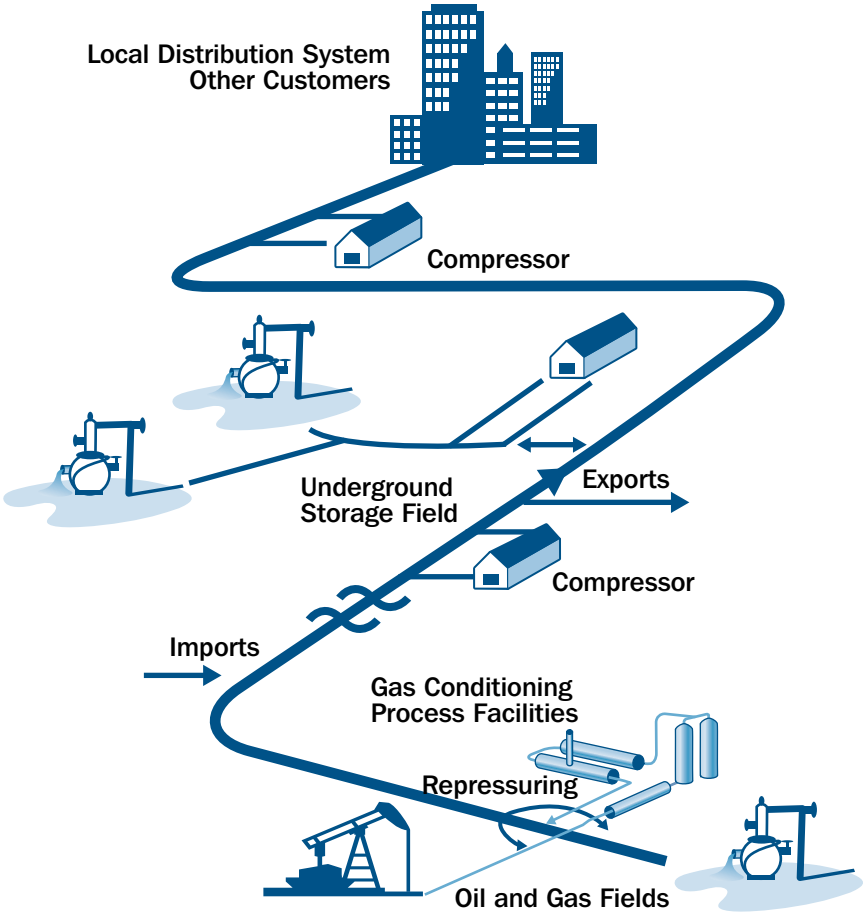
Natural gas provided 23 percent of U.S. energy needs in 2005, and its use is growing.[17] In particular, power producers and industrial facilities are opting for gas-powered equipment, and residential customers use natural gas for heating and cooking.

Figure 1-6: 2005 Natural Gas Statistics

Production	405,048 gas and condensate wells (2004)
Gathering	24,000-plus miles of gathering pipeline
Processing	530 gas processing plants (lower 48 States, 2004)
Transmission	304,000 miles of interstate natural gas and petroleum pipeline
Storage	394 underground storage facilities 8.3 trillion cubic feet capacity 96 LNG storage facilities
Distribution	1.9 million miles of intrastate pipeline

Sources: Production, processing, and storage data from EIA; gathering, transmission, and distribution from Pipeline and Hazardous Material Safety Administration's Pipeline Safety Program.

Figure 1-7: Flow of Natural Gas



[17] EIA, *Annual Energy Review* 2005, table 1.3. www.eia.doe.gov/emeu/aer/txt/stb0103.xls.

Although most of the gas consumed in the United States is produced domestically, imports have increased from 8.0 percent of consumption in 1990 to 19.7 percent in 2005 (table 1.3).[19] This trend is likely to continue over the next few years as imported LNG assumes a larger role in the market supply.

Table 1.3: Natural Gas Import Dependence, 2005[18]

U.S. Production	18.2 trillion cubic feet
Net Imports	3.7 trillion cubic feet pipeline gas 0.6 trillion cubic feet LNG
Import Dependence	19.7 percent

1.2.3.1 Natural Gas Production, Processing, Transport, Distribution, and Storage

Natural gas production. Federal Offshore Gulf of Mexico and Texas are the largest gas-producing regions in the United States, at approximately 11 billion and 13 billion cubic feet per day, respectively.[20] The two regions account for almost half of all U.S. natural gas production. The United States had 193 trillion cubic feet of dry natural gas reserves as of December 31, 2004.[21]

Natural gas processing. Natural gas processing consists of separating all of the various hydrocarbons and fluids from the pure natural gas to produce pipeline-quality dry natural gas. Most U.S. natural gas processing plants are located near production facilities in the Southwest and Rocky Mountain States. The natural gas extracted from a well is transported to a processing plant through a network of gathering pipelines.

Natural gas transportation. The interstate natural gas pipeline network transports natural gas from processing plants in producing regions to areas with high natural gas requirements, particularly large urban areas. Compression stations along the pipeline transmission route keep the gas moving at the desired pressure.

Natural gas distribution. Local distribution companies typically transport natural gas from interstate pipeline delivery points to end users through thousands of miles of distribution pipe. Delivery points for local distribution companies are often termed city gates, especially for large municipal areas, and are important market centers for the pricing of natural gas.

Natural gas storage. Gas is typically stored underground and under pressure as an efficient way to balance discrepancies between supply input and market demand. Three types of facilities are used for underground gas storage: depleted reservoirs in oil and/or gas fields, aquifers, and salt caverns. Facilities serving the interstate market are subject to Federal Energy Regulatory Commission (FERC) regulations; otherwise they are State-regulated. Most working gas held in storage facilities is held under lease with shippers, local distribution companies, or end users who own the gas.

1.2.3.2 Liquefied Natural Gas Facilities

LNG is produced by cooling natural gas to –260 degrees Fahrenheit (–160 degrees Centigrade). In its liquid state, natural gas occupies 618 times less volume than the same mass of gaseous methane at standard conditions, which allows it to be transported by specially designed ships or tankers. The lower 48 States have 5 marine terminals for receiving, storing, and regasifying LNG for delivery into the pipeline network, and more than 50 above-ground LNG storage tanks for meeting peak-day demand.

1.2.3.3 Natural Gas Control Systems

To monitor and control the flow of natural gas, centralized gas control stations collect, assimilate, and manage data received from compressor stations all along the pipeline. These control systems can integrate gas flow and measurement data with other accounting, billing, and contract systems.

[18] EIA, Natural gas production: http://tonto.eia.doe.gov/dnav/ng/ng_prod_sum_dcu_NUS_a.htm; natural gas imports by country: http://tonto.eia.doe.gov/dnav/ng/ng_move_impc_s1_a.htm; import dependence calculated from total consumption: www.eia.doe.gov/emeu/aer/txt/stb0605.xls.

[19] EIA, *Annual Energy Review* 2005, tables 6.2 and 6.3. www.eia.doe.gov/emeu/international/gastrade.html.

[20] EIA, http://tonto.eia.doe.gov/dnav/ng/ng_prod_sum_a_EPG0_FPD_mmcf_a.htm.

[21] EIA, http://tonto.eia.doe.gov/dnav/ng/ng_enr_sum_dcu_NUS_a.htm.

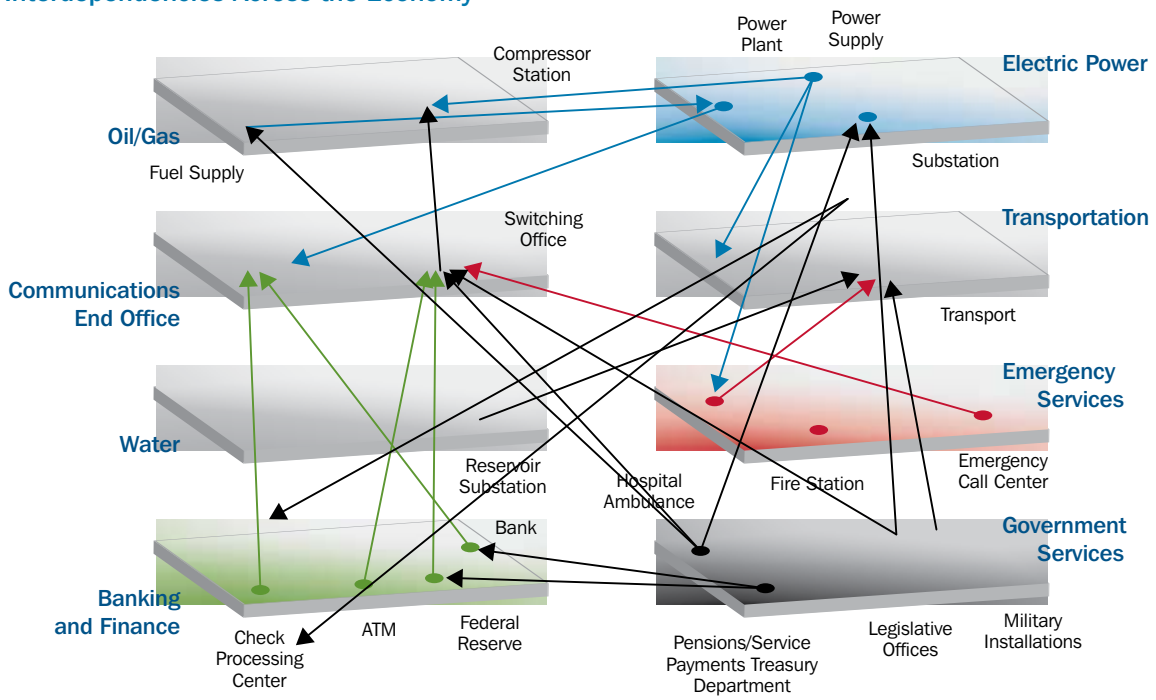
1.2.3.4 Gas Market Centers

Currently, 37 natural gas market centers operate in the United States and Canada. These centers provide gas shippers with many of the physical capabilities and administrative support services formerly handled by interstate pipeline companies as bundled sales services (e.g., physical coverage of short-term receipt/delivery balancing needs). These centers have developed new and unique Internet-based access to gas trading platforms and capacity release programs; provide title transfer services between parties that buy, sell, or move their gas through the centers; and offer connections with other pipelines and access to storage services. These markets and their information systems are critical components of the natural gas infrastructure.

1.2.4 Energy Sector Interdependencies

Sector interdependencies. During the last half of the 20th century, technical innovations and developments in digital information and telecommunications dramatically increased interdependencies among the Nation's critical infrastructures. As shown in figure 1-8, each infrastructure depends on other infrastructures to function successfully. Disruptions in a single infrastructure can generate disturbances within other infrastructures and over long distances, and the pattern of interconnections can extend or amplify the effects of a disruption. The energy infrastructure provides essential fuel to all of the other critical infrastructures, and in turn depends on the Nation's transportation, communications, finance, and government infrastructures. For example, coal shipments are highly dependent on rail. There are also interdependencies within the energy infrastructure itself, particularly the dependence of petroleum refineries and pipeline pumping stations on a reliable electricity supply and backup generators and utility maintenance vehicles to be supplied with diesel and gasoline fuel.

Figure 1-8: Interdependencies Across the Economy



International interdependencies. Energy infrastructure interdependencies also cross international borders. Oil and natural gas pipelines and electric transmission lines have helped integrate the energy systems of North America. Moreover, increasing imports of petroleum products continue to highlight the dependence of the United States on foreign oil.

1.3 Security Partners

No single government agency, industry group, or company can secure the entire energy infrastructure. Collaboration at all levels is essential to securing an interdependent infrastructure that is owned, operated, hosted, and regulated by many entities. Voluntary partnerships help facilitate the useful exchange of security-related information and maximize the effectiveness of infrastructure protection efforts. DOE is working to coordinate critical energy infrastructure protection and resiliency efforts with private, government, and international partners. The Energy SSP provides the basis for close and effective coordination among all sector security partners.

1.3.1 Relationships With Industry Owner/Operators and Organizations

1.3.1.1 Sector Coordinating Councils

As defined in the 2006 NIPP Base Plan, SCCs are created by owners and operators and are self-organized, self-run, and self-governed, with a spokesperson designated by the sector membership who serves as the principal for coordinating with the Federal Government on a wide range of CI/KR protection activities and issues.[22]

The Energy Sector established two SCCs in 2004 to help coordinate ongoing industry initiatives, government partnerships, and responsibilities. The Electricity SCC (ESCC) represents more than 95 percent of electricity industry owners and operators and includes representatives from more than 30 industry organizations. It also includes the executive committee of NERC's Critical Infrastructure Protection Committee (CIPC), along with the president and chief executive officer of NERC.[23] The Oil and Natural Gas SCC (ONG SCC) represents more than 98 percent of ONG sector owners and operators with representatives from 22 industry trade organizations. The council chairperson acts as the prime contact for DHS. The members of the ONG SCC also work on transportation sector pipeline efforts.

DOE works at many levels with the electricity, petroleum, and natural gas industries. It interacts with numerous trade associations and industry groups to share information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security.

1.3.2 Relationships With Government Agencies

1.3.2.1 Government Coordinating Council

The government counterpart for the SCCs is the Energy Sector GCC, which was also established in early 2004. The GCC is co-chaired by DOE and DHS, and is composed of representatives across various levels of government (Federal, State, local, or tribal) that are concerned with the security of the Energy Sector.[24] The members of the Energy Sector GCC also work on Transportation Systems Sector pipeline efforts.

1.3.2.2 Relationships With Other Federal Departments and Agencies

DOE has longstanding relationships with a number of Federal agencies to help fulfill its mission to provide safe and secure energy supplies. A number of these agencies have critical responsibilities regarding the Energy Sector (see appendix 3, which provides a brief summary of Federal legislative authorities related to the Energy Sector). For example:

- **Department of Agriculture (USDA).** DOE coordinates with USDA's Rural Utilities Service, which provides funding and support for rural electric utilities.
- **Department of Defense (DOD).** DOE coordinates with the USACE regarding maintenance of the Nation's dams.

[22] DHS, 2006 *National Infrastructure Protection Plan Base Plan*, section 4.1.2.3, p. 54.
[23] NERC, www.nerc.com/~filez/cip.html.
[24] 2006 *National Infrastructure Protection Plan Base Plan*, section 4.1.2.3, p. 54.

- **Department of Homeland Security (DHS).** DOE works with DHS, which leads, integrates, and coordinates CIP activities across the Federal Government. As previously noted, certain segments of the Energy Sector are directly coordinated by DHS, including nuclear power and hydroelectric power (dams). The DHS Transportation Security Administration oversees pipeline security and works closely with the Department of Transportation (DOT) and DOE on matters where pipeline safety and security overlap. DOE works closely with the Federal Emergency Management Agency (FEMA) to address natural disasters and security issues related to the provision of energy and public safety. The United States Coast Guard (USCG) has protective responsibility for offshore oil and gas facilities, and for implementing regulations under the Maritime Transportation Security Act that impact Energy Sector facilities.[25] DOE also coordinates with USCG regarding problems at terminals and waterways. DOE is working with DHS to coordinate current and future threat identification and assessment, mapping threats against U.S. vulnerabilities, issuing timely warnings, and taking preventive and protective action. DOE is also working with the DHS Office of Cyber Security and Communications to address and enhance the security of the sector's cyber infrastructure through such efforts as the Control Systems Security Program. DHS is responsible for implementing chemical security regulations that will impact some important Energy Sector assets.
- **Department of the Interior (DOI).** DOE coordinates with DOI's U.S. Geological Survey regarding coal mines and geothermal production areas and power plant siting. DOE, through the Power Marketing Administrations (PMAs), also coordinates power generation and river operations with DOI's BOR on hydrogeneration projects. It also coordinates with DOI's Minerals Management Service (MMS), which manages the Nation's natural gas, oil, and other mineral resources on the Outer Continental Shelf.
- **Department of State (DOS).** Energy is imported and exported each day. DOE works with other agencies on energy movements across U.S. borders with Canada and Mexico, and cooperates through international agreements led by the DOS and DHS.
- **Department of Transportation (DOT).** The Energy Sector relies on pipelines, barges, tankers, railways, and highways to transport all raw and refined energy products. DOE is already coordinating activities regarding oil and natural gas pipelines with DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA), and is a member of the interagency committee charged with developing a memorandum of understanding (MOU) to facilitate prompt repair of oil and natural gas transmission pipelines.
- **Environmental Protection Agency (EPA).** EPA is responsible for enforcement of the Clean Air Act. DOE coordinates with EPA during energy emergencies and supply disruptions to assess the availability of transportation and boutique fuels and the need for environmental fuel waivers. DOE also coordinates with EPA on air quality and fuel-related emissions.
- **Federal Energy Regulatory Commission (FERC).** FERC is an independent agency that regulates the interstate transmission of natural gas, oil, and electricity, as well as natural gas and hydropower projects. FERC oversees approval of electric reliability standards and enforcement of those standards, which are developed by NERC in its capacity as the Energy Reliability Organization (ERO) under the Energy Policy Act of 2005. FERC can also impose safety requirements to ensure or enhance the operational reliability of the LNG facilities within its jurisdiction. DOE coordinates with FERC on energy security issues.
- **Nuclear Regulatory Commission (NRC).** DOE will continue to coordinate with NRC on energy security issues related to electricity generated by nuclear fission, relying on the experience gained from DOE's own operation of numerous nuclear facilities.

1.3.2.3 Relationships With State, Local, and Tribal Agencies

States and local governments are crucial stakeholders in providing a secure and reliable energy infrastructure for the Nation. State and local government agencies are responsible for emergency planning and response, developing energy security and reliability policies and practices, and facilitating Energy Sector protection activities. They are the organizations that citizens turn to in times of crisis, and they play a significant role in preventing energy supply crises and mitigating the impacts of emergencies

[25] The U.S Coast Guard, the Federal Energy Regulatory Commission, and DOT's Pipeline and Hazardous Materials Safety Administration coordinate to address marine safety and security at LNG import facilities.

that do arise. DOE has established liaisons with State and local government agencies responsible for preventing and responding to energy disruptions. DOE will continue to strengthen these relationships with specific initiatives described in chapter 5, State and local organizations that play roles in Energy Sector security and assurance include the following:

- State government energy offices, represented by the National Association of State Energy Officials (NASEO), typically serve many energy-related functions at the State level, including coordinating responses to energy emergencies, developing energy emergency plans, and developing practices to improve energy security and reliability. This work is coordinated by NASEO's Energy Data and Security Committee.
- State public utility commissions, represented by the National Association of Regulatory Utility Commissioners (NARUC), are agencies engaged in the regulation of utilities (energy, water, telecommunications) at the State level. In this role, these organizations are involved in cost-recovery issues (including energy security costs), energy supply curtailment plans, emergency response, and CIP activities. NARUC's Committee on Critical Infrastructure is the focal point for this effort.
- Governors' offices and State legislators, represented by the National Governors Association (NGA) Center for Best Practices and the National Conference of State Legislatures (NCSL), respectively, develop policies that affect energy security and assurance and play major roles in responding to energy emergencies. These State-level decisionmakers coordinate with Federal and industry groups on energy security and emergency issues, and possess emergency authorities they can exercise to mitigate the impacts of energy crises.
- State Homeland Security Directors and their offices coordinate and conduct homeland security activities at the State level, including programs involving infrastructure protection and vulnerability analysis.
- State and local emergency management agencies, represented by the National Emergency Management Association (NEMA), and first responders prepare for and respond to all emergencies, including those with implications for the energy infrastructure. These organizations are on the front lines of emergency response at the State and local levels.
- Local governments and associations that represent them comprise an extremely large set of stakeholders that represent the interests of cities, towns, and municipalities in Energy Sector security, protection, and emergency preparedness.
- Tribal agencies play significant roles in electricity transmission corridors, especially in the Southwest, and in various energy supply resources including coal and potentially in the growth of wind and other renewable energy sources.[26]

State and local governments are required under Federal homeland security funding guidance to implement the NIPP, as well as the National Response Plan (NRP) and National Incident Management System. As State and local governments develop their critical infrastructure plans, each Governor has designated a State Administrative Agency (SAA) to support development of homeland security strategies, implement strategic goals and objectives, and administer Federal preparedness assistance. States may wish to identify State agencies as sector leads, much as the Federal Government has identified SSAs in certain cases. This would parallel the approach taken in HSPD-7 at the State level. For example, State public utility commissions are responsible for the cost recovery of utility investment in critical infrastructure, and many are responsible for emergency response and gas pipeline safety. Many State energy offices have expertise in the petroleum infrastructure, monitor petroleum supply and demand, and provide for emergency response as well.

At the national level, the Energy Emergency Assurance Coordinators (EEAC) system is a cooperative effort among NASEO, NARUC, NCSL, NGA's Center for Best Practices, the Public Technology Institute, and DOE's Infrastructure Security and Energy Restoration Division (ISER). The system establishes a secure cooperative communications environment for State and local government personnel with access to information on energy supply, demand, pricing and infrastructure. Designated members have expertise in electricity, petroleum, and natural gas. The current membership of approximately 180 is composed of repre-

[26] See Council of Energy Resource Tribes at www.certredearth.com.

sentatives from State energy offices, public utility commissions, State legislatures, emergency management agencies, homeland security offices, and governors' offices. The EEAC system is housed on DOE's ISERnet Web site.[27]

1.3.2.4 Interaction and Communication Among Private and Public Sectors

Critical Infrastructure Protection Advisory Council (CIPAC). DOE also works in partnership with CIPAC, established by DHS as part of the NIPP. CIPAC facilitates interaction among government representatives and representatives of CI/KR owners and operators in each sector.

Information Sharing and Analysis Center. DOE collaborates with the sector's use of the Electricity Sector Information Sharing and Analysis Center (ESISAC)[28] and the Homeland Security Information Network (HSIN).[29] (See chapter 5 for a more complete description.) ESISAC and HSIN provide mechanisms by which the energy industry can share and analyze important information about vulnerabilities, threats, intrusions, and anomalies, and through which it can communicate with and provide support to the Federal Government. Both ESISAC and ONG-HSIN can be used to share information with other critical infrastructures. In addition, DOE's secure ISERnet Web site contains the Energy Industry Assurance Coordinators (EIAC) system, a database of key industry personnel who can exchange information with DOE during energy emergencies. The site provides threat awareness and relevant security analyses and presentations.

1.4 Value Proposition

Efficiently and effectively securing the Energy Sector necessitates significant investment from all security partners. These investments require expenditures of time, energy, money, and other resources. While these expenditures typically are executively or legislatively mandated for government, private sector participation is mostly voluntary. Beyond existing regulatory requirements, participation by the private sector has been significant in the Energy Sector. Compelling reasons for private sector security partners to participate include opportunities to:

- Share credible, timely, actionable threat information and predictive/trend analyses where possible;
- Apply a risk-based and prudent business approach for protecting assets that builds on existing industry practices and methodologies;
- Support flexible allocation of protective resources based on threats, consequences, and vulnerabilities;
- Improve risk management through exposure to effective practices and risk management tools;
- Provide a forum for reaching out to peers and addressing interdependencies;
- Provide a platform for coordination and communication between government and industry regarding protective actions and risk management activities;
- Build and further strengthen existing trusted relationships with private and public sector partners; and
- Inform government regarding impediments to protecting energy assets.

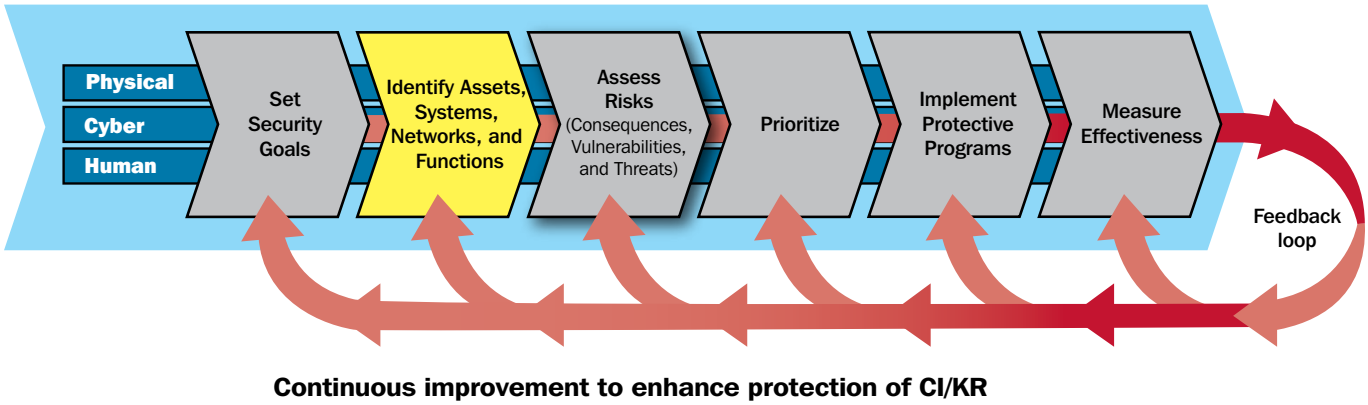
[27] ISERnet is an Internet community of Federal, State, and local government and industry professionals who share in the effort to protect CI/KR in the Energy Sector and ensure a secure and reliable flow of energy. DOE's Office of Electricity Delivery and Energy Reliability/Infrastructure Security and Energy Restoration established this secure communication environment to address energy emergencies and supply disruptions and share timely information. The site contains two separate systems: the EEAC system for State and local governments, and the EIAC system for industry personnel.

[28] ESISAC, www.esisac.com.

[29] HSIN is managed by the Homeland Security Operation Center, www.dhs.gov/dhspublic/display?theme=30&content=3813. ONG-HSIN replaced ESISAC in August 2006.

2. Identify Assets, Systems, Networks, and Functions

Figure 2-1: Identify Assets, Systems, Networks, and Functions



This chapter discusses the ongoing efforts by industry, and as appropriate by government security partners, to identify Energy Sector assets, systems, networks, and functions that could, if compromised, result in significant economic damage or human casualties. It also discusses relevant information parameters and existing data sources that are available to help the Energy Sector conduct risk management activities and protect infrastructure assets and systems.

2.1 Defining Information Parameters

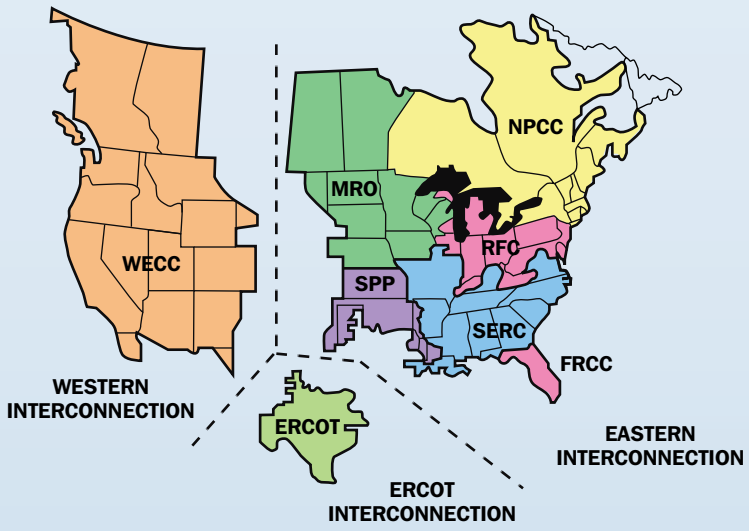
2.1.1 Energy Assets and Systems

Broadly speaking, Homeland Security Presidential Directive 7 (HSPD-7) defines the Energy Sector as the Nation's electric system (excluding nuclear power plants and hydroelectric dams), natural gas system, and petroleum/petroleum product systems. Figure 2-2 describes the operation of the electric grids in North America. As discussed in chapter 1, these three energy systems are highly interdependent (e.g., natural gas is a significant fuel for electric generation) and are critical for other infrastructure sectors, including Communications, Drinking Water and Water Treatment Systems, Chemical, Information Technology, and Transportation Systems. Each of these interdependent energy systems consists of many individual assets, which in some cases may be highly important, but their importance varies dramatically depending on factors such as time of day, time of year, and system conditions. From a reliability and security perspective, however, systems are the critical characteristic of the Energy Sector.

Figure 2-2: Reliable Operation of the North American Electric Power Grid System

While the power system in North America is commonly referred to as "the grid," there are actually four distinct power grids or "interconnections". The Eastern Interconnection includes the eastern two-thirds of the continental United States and Canada from Saskatchewan east to the Maritime Provinces. This excludes Quebec Province, which is its own interconnection, the fourth in North America. The Western Interconnection includes the western one-third of the continental United States (excluding Alaska), the Canadian provinces of Alberta and British Columbia, and a portion of Baja California Norte, Mexico. The third interconnection comprises most of the State of Texas. The interconnections are electrically independent from each other except for a few direct current (DC) ties that link them. Within each interconnection, electricity is produced the instant it is used and flows over virtually all transmission lines from generators to loads.

The four power grids form an integrated system that has been described as the world's largest machine. It is made up of literally hundreds of thousands of interconnected generators, transmission lines, and substations. Each of these individual components are designed and operated within the parameters necessary to assure integrated grid reliability. Reliable operation of the power grid is achieved by addressing two fundamental characteristics of electricity.



The electricity grid that serves the continental United States and Canada is actually four separate systems.

First, electricity flows at close to the speed of light and is not economically storable in large quantities. Therefore, electricity must be produced the instant it is used, and the system must be managed every second of the day to monitor and respond to changes very quickly.

Second, electricity flows freely along all available alternating current (AC) paths from the generators to the loads according to the laws of physics, dividing among all connected flow paths in the network. These multiple paths provide resiliency to instantly respond to both planned and unexpected equipment outages in the system.

Maintaining reliability requires trained and skilled operators, sophisticated computers and communications, and careful planning and design. NERC and its eight Regional Reliability Councils have developed system operating and planning standards, based on seven key concepts, for ensuring the reliability of the four grids:

1. Balance power generation and demand continuously.
2. Balance reactive power supply and demand to maintain scheduled voltages.
3. Monitor flows over transmission lines and other facilities to ensure that thermal (heating) limits are not exceeded.
4. Keep the system in a stable condition.
5. Operate the system so that it remains in a reliable condition even if a contingency occurs, such as the loss of a key generator or transmission facility (the "N-1 criterion").

6. Plan, design, and maintain the system to operate reliably.
7. Prepare for and respond to emergencies.

Planning and operating standards are reinforced through compliance audits, sanctions, and penalties that will be enforceable across North America as NERC evolves to fulfill its role as the ERO. Some State public utility commissions may also have a role in assuring reliable operation of the power grid.

2.1.2 Defining Energy Asset and System Parameters

The Energy Sector has identified six general asset or system characteristics that are important parameters for evaluating the vulnerabilities of the Energy Sector infrastructure and developing risk management programs.

- **Physical and location attributes.** These assist the Energy Sector to develop consequence, vulnerability, and protective strategies.
- **Cyber Attributes.** Cyber systems help monitor and control the energy systems.
- **Volumetric or throughput attributes.** These define the extent of the damage, depending on the utilized capacity of the system, or points where the system may be capacity constrained.
- **Temporal/load profile attributes.** The Energy Sector has a strong temporal or time-dependent dimension affected by the season of the year and/or time of day.
- **Human attributes.** Highly trained and skilled personnel are key factors in a comprehensive Energy Sector security plan. The availability of skilled and experienced technical talent is a concern in the Energy Sector. Sustaining essential technical knowledge is critical to maintaining the sector's safety, reliability, and security.
- **Importance of asset or system to the energy network.** Disruption of a particular gas pipeline or storage facility could impact the ability of power generation assets to function properly.

2.1.3 Information Collection and Sharing

The Energy Sector already has considerable data available to support a wide range of consequence, risk, and vulnerability assessments. These data are collected and used by owners, operators, trade associations, and a variety of industry organizations. In addition, the Government collects a wide variety of Energy Sector information, principally through the authorities of various Federal agencies[30] and at the State and local levels through authorities of public utility commissions, State energy offices, and State and local homeland security initiatives. Established communication links also exist between Federal, State, and local government representatives and industry.

The Energy Sector recognizes that, during times of increased security posture or emergency situations, the best information sources are the trusted relationships between government and industry. Such relationships ensure that necessary information is provided when and where it is needed and can be directly applied to protect and recover key energy infrastructure and resources. Established relationships between industry and all levels of government and other key stakeholders will be relied on where necessary to facilitate information flow, through HSIN and other information-sharing mechanisms. Further, energy security partners will continue to communicate with DHS regarding additional needs, information resources, and database

[30] For example, FERC, EIA, DOE, DOT, DHS, TSA, and USCG.

approaches required to support DHS programs. State energy emergency preparedness and response plans highlight the identification of assets and the role of State government officials, in conjunction with their private sector counterparts, in addressing various levels of an energy emergency.

The Energy Sector also has a long history of mutual aid and support that can be relied on in emergency situations. This aid is largely focused on emergency response and recovery to support restoration of service to customers. Regional planning groups in the natural gas and electricity industries plan for regional reliability and often conduct exercises to prepare for energy emergencies. States also conduct regional energy emergency exercises involving the private sector to assure coordinated responses across State borders and with the private sector.

2.1.4 Existing Energy Sector Information Resources

As stated previously, the Energy Sector already has very substantial information sources available to support CI/KR protection, planning, and analysis. The following sections describe the types of information used by the Energy Sector.

2.1.4.1 Electric Generation and Transmission Information

Electric generation and transmission assets are grouped into existing and new plants and facilities. Because of the long lead times to build a new power plant or transmission line and bring it on line, tracking of new facilities in various stages of development is performed by the industry. Major attributes include location, capacity, and ramp-up or black start times, as well as electrical location on the grid (in terms of voltage support and similar grid stability metrics). These attributes relate directly to operators' abilities to maintain power production to meet demand through both scheduled and unscheduled plant outages.

2.1.4.2 Petroleum Asset Information

Physical petroleum asset data, including location and throughput data, are maintained by both industry and government. These data are important in assessing the consequences and vulnerability of the various types of petroleum assets. As with electricity, data on petroleum control systems and markets/trading platforms are also maintained.

2.1.4.3 Natural Gas Asset Information

Government and industry both maintain natural gas asset data. Natural gas systems also employ SCADA-type control systems and markets/trading platforms for which asset data are maintained. Natural gas markets have existed for some time, and both physical and financial products are traded. A key platform is the New York Mercantile Exchange (NYMEX).

FERC requires the annual filing of system flow diagrams by jurisdictional companies.[31] These filings contain data for facilities that were installed or operated during the reporting year and include miles of pipeline, diameter of each section, maximum allowable operating pressures of each segment, direction of flow, total horsepower at each compressor station, daily and seasonal withdrawal volumes at each storage field, and volume delivered to each customer.

Another filing requirement instructs jurisdictional companies to notify FERC of all serious service interruptions lasting longer than 3 hours.[32] Reports must be filed at the earliest possible time following the interruption and must include the location, time, and number of customers affected, as well as any emergency measures taken to remedy the situation.

2.1.4.4 Protection of Collected Data

The Energy Sector expects that all data and information voluntarily provided to DHS or DOE by industry will be protected from release by Protected Critical Infrastructure Information (PCII) or other appropriate classification procedures. The Energy Sector will work with the PCII Program Office within the DHS Office of Infrastructure Protection (OIP) to apply provisions of the CII Act, and the implementing regulations contained in 6 CFR Part 29, to critical infrastructure information that is not

[31] As specified in 18 CFR 260.8.
[32] As specified in 18 CFR 260.9.

customarily in the public domain and is voluntarily submitted to DHS. Other government sector security partners will work to protect sensitive information from unintended release. The Energy Sector will also work with State, local, and tribal authorities to ensure that information provided to those non-Federal authorities is also appropriately protected from release and not used for purposes other than infrastructure protection and recovery. Through NARUC, States are developing models for information sharing and protection in the State regulatory context, and public utility commissions are engaging in training and network-building that will enable each State to provide the right information to the right parties when needed.

2.2 Collecting Infrastructure Information

DOE and Energy Sector partners may need to initiate data collection for this SSP beyond what currently exists. Large CIP-focused data collection efforts on the part of government agencies are not required because the Energy Sector already has considerable data to help analyze consequences and vulnerabilities and to develop protective and resiliency strategies. However, when appropriate, DOE will work with sector security partners to obtain and appropriately protect additional information from industry, government, and other stakeholders. The Energy Sector will also work and coordinate with other sectors where dependencies and interdependencies exist.

For State and local efforts, some additional information may also be needed on critical energy infrastructure in their jurisdictions so that they understand risk, vulnerabilities, and consequences, and can properly set their priorities for protective measures that will support and complement the private sector efforts.

2.3 Verifying and Updating Infrastructure Information

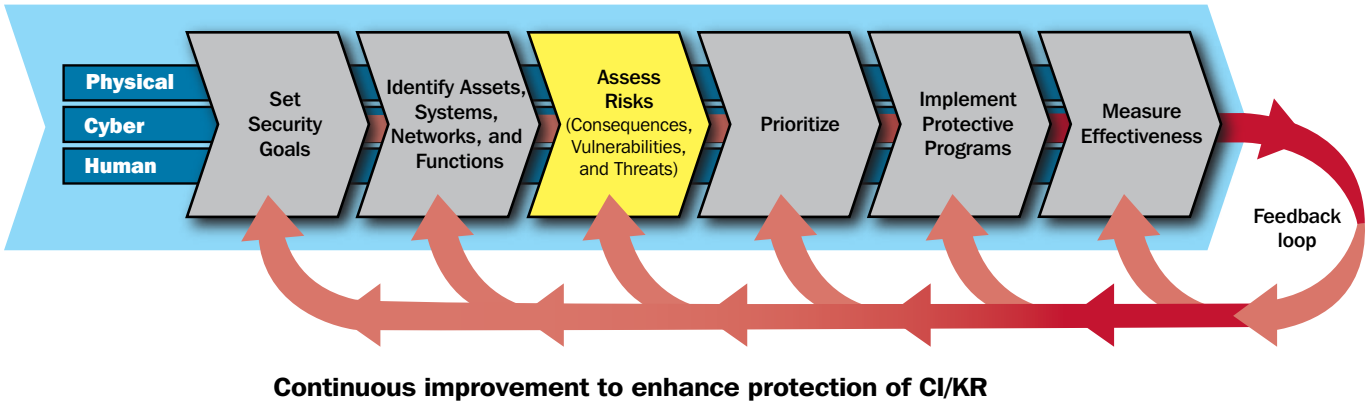
Many of the existing data used by the Energy Sector are already subject to verification and validation protocols. For example, EIA maintains a rigorous data verification and validation program for the data it collects from industry. Many State commissions, FERC, and NRC also conduct data and management audits of reporting companies because the data are used for regulatory and ratemaking purposes. TSA has an ongoing program in which data on pipeline security programs are collected and evaluated. Where existing data verification processes are deemed inadequate, the Energy Sector will work with expert groups to identify and implement appropriate processes, including processes to verify cyber-related data.

The Energy Sector will ensure that all data used for CIP purposes are verified, fill a clearly identified void, meet mutually agreed-upon accuracy and completeness thresholds, and are essential to energy infrastructure protection. In emergencies or crises, trusted communication channels among Energy Sector security partners will be used to help ensure data quality.

The Energy Sector will support the updating of key energy asset and infrastructure data, making use of the existing update procedures of data-collecting organizations.

3. Assess Risks

Figure 3-1: Assess Risks



This chapter describes the Energy Sector's current approaches for assessing risk. As defined in the NIPP Base Plan, risk is a measure of potential harm that encompasses threat, vulnerability, and consequence. That is:

$$\text{Risk (R)} = f(C, T, V)$$

where an asset's risk is a function of the likely consequences (C) of a disruption or successful attack; the likelihood of a disruption or attack on the asset, often referred to as the threat (T) to the asset or the asset's attractiveness; and the asset's vulnerability (V) to a disruption or attack. As discussed in the sections below, the Energy Sector uses a variety of approaches that apply this widely accepted risk management principle to assess risk.

3.1 Use of Risk Assessment in the Sector

The Energy Sector has extensive experience in development and application of methodologies for assessing facility and system risk and prioritizing assets to be protected. Such methodologies have been developed by a variety of sector security partners, including individual energy companies that own and operate Energy Sector assets; professional and trade associations; academic institutions; research centers; and DOE, as an integral part of meeting its longstanding responsibilities for safety and security and implementing its CIP program for the Energy Sector.

Because of the diversity of assets in the Energy Sector, many risk assessment methodologies are used. Some methodologies are tailored to a specific segment of the sector (i.e., electricity, oil, natural gas, or their system components), while others are used to assess risks at the system or sector level. In addition, some have broad applicability that extends across multiple CI/KR sectors.

Many of the methodologies used in the Energy Sector include dependencies with and interdependencies among infrastructures. The energy industry sponsors and participates in regional and national planning activities that are designed to identify and understand system and interdependency considerations that transcend individual companies and that may be used by DHS during national emergencies to prioritize efforts. The Energy Sector has been actively engaged in exercises to develop response strategies involving multiple agencies, companies, and governmental entities. The Energy Sector will continue to develop ties to other sectors and explore the extent and importance of interdependencies.

The broad range of methods used by the Energy Sector to assess risk also results from the international scope of the sector's assets, supply chains, and products. Many energy companies are global and have extensive experience in dealing with a wide variety of natural and manmade threats. This experience has resulted in effective ways to prioritize security investments based on risk. It has also highlighted the importance of interdependencies within the sector as well as among the other CI/KR sectors.

DOE, in cooperation with sector security partners, has undertaken programs to assess the risks of key energy infrastructure assets and to provide technology, tools, and expertise to other Federal, State, and local organizations and the private sector. These programs have involved establishing partnerships with infrastructure owners/operators, State and local governments, and a wide range of industry associations. Products include vulnerability and risk assessment-related methodologies, checklists, lessons learned, support for policy analysis, and guidelines for various types of assets. DOE's efforts are designed to assist all entities within the energy infrastructure in securing systems against physical and cyber attacks.

The Energy Sector also has worked closely with DHS in developing and transferring risk assessment methodologies. The sector has participated in DHS's Buffer Zone Protection Program (BZPP) and has worked with it to develop Risk Analysis and Management for Critical Asset Protection (RAMCAP) modules for petroleum refining and LNG facilities. Further testing and evaluation by the sector will be needed to determine the effectiveness of these modules, which are designed to compare the risks associated with one refining or LNG facility to another and to support in-sector and DHS cross-sector risk comparisons. Given the diversity of facilities in the Energy Sector and the wide range of methodologies being used successfully to assess risk, a "one size fits all" risk assessment solution is not appropriate.

A set of baseline criteria for the methodologies used to support all levels of comparative risk analysis is defined in the NIPP Base Plan.[33] The Energy Sector will consider such criteria through the Critical Infrastructure Protection Advisory Council (CIPAC) as the sector evaluates how best to move forward in terms of vulnerability and/or risk assessments that will support DHS's national risk analysis goals and to improve these methodologies.

[33] See NIPP Base Plan, appendix 3A.

3.2 Screening Infrastructure

As discussed in chapter 1, the Energy Sector consists of many thousands of electricity, oil, and natural gas assets, which are connected in systems and networks. Screening methodologies help identify which assets are significant for further assessment. That is, they enable a determination of the need for a more detailed vulnerability or risk assessment. In light of the large number of energy facilities and assets spread throughout the Nation, many of which may pose little or no security risk, as well as the limited resources available to address their security, it is neither practical nor financially responsible to perform comprehensive risk assessments of all assets or facilities. Thus, as a precursor to indepth risk assessment efforts, screening is used to identify which facilities warrant expenditure of additional resources.

Many screening approaches are used by energy companies to prioritize facilities for more rigorous assessments. These approaches commonly focus on health and safety consequences as well as broad-based economic consequences. Energy industry associations have developed and disseminated security guidelines to help screen assets and assess risks in oil, natural gas, and electricity infrastructure.

The electric grid operators utilize their energy management systems to run sophisticated contingency analysis programs every 5 to 10 seconds to identify the most critical components of the electric systems. The operators are always aware of the critical assets of the grids and the consequences if a key component is removed from service, and operate the system to mitigate the loss of the key components.

In addition to the current screening processes used by industry, the Energy Sector, in conjunction with DHS, is developing and testing "Top Screens" for petroleum refining and LNG facilities. These consist of screening questions that are intended to filter out facilities that are low national security risks because of the nature of their business, their location or lack of proximity to significant population groups or other critical infrastructure, or relatively limited importance to the national economy or military capability.[34]

The industry, in cooperation with governmental Energy Sector partners, will discuss common approaches and next steps to refine approaches and to share experiences, commonalities, and effective practices in the use of screening tools. This will involve industry security committees as well as SCCs and key governmental participants.

3.3 Assessing Consequences

The potential physical and cyber consequences of any incident, including terrorist attacks and natural or manmade disasters, is the first factor to be considered in risk assessment. In the context of the NIPP Base Plan, consequence is measured as the range of loss or damage that can be expected.

The consequences that are considered for the national-level comparative risk assessment are based on the criteria set forth in HSPD-7. These criteria can be divided into four main categories:

- **Human Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Direct and indirect effects on the economy (e.g., costs resulting from disruption of products or services, costs to respond to and recover from the disruption, costs to rebuild the asset, and long-term costs due to environmental damage);
- **Impact on Public Confidence:** Effect on public morale and confidence in national economic and political institutions; and
- **Impact on Government Capability:** Effect on government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

[34] For example, one DOE PMA, the Bonneville Power Administration (BPA), has used the following screening criteria to identify its most critical facilities: economic security, national security, public health and safety, generation, and regional and national grid reliability.

An assessment of all categories of consequence may be beyond the capabilities available for a given risk analysis. Most Energy Sector assets are not associated with mass casualties, but may have economic and long-term health and safety implications if disrupted. However, the redundancy of system-critical facilities and overall system resilience minimize the potential for such consequences.

The complexity, diversity, and interconnectedness of the Energy Sector dictate the need for assessing consequences at many different levels of detail:

- Asset or facility level;
- System, sector, and urban area level; and
- Regional and/or national level.

These assessments must consider interdependencies within the Energy Sector and among the other CI/KR sectors at all levels. These interdependencies may have national, regional, State, and/or local implications and are considered to be an essential element of a comprehensive examination of physical and cyber vulnerabilities.

DOE, as the Energy SSA, and the Energy Sector SCCs will coordinate with DHS, DOT, NRC, and other Federal organizations with responsibilities under HSPD-7 as appropriate to ensure that assessments are conducted in a timely manner. Coordination between DOE and States will ensure that these efforts are coordinated with State activities and initiatives.

3.4 Assessing Threats

The Energy Sector views threat analysis broadly, encompassing natural events, criminal acts, insider threats, and foreign and domestic terrorism. Natural events are typically addressed as part of emergency response and business continuity planning. In the context of risk assessment, the threat component of risk analysis is calculated based on the likelihood that an asset will be disrupted or attacked. Such information is essential for conducting meaningful vulnerability and risk assessments. Therefore, the Energy Sector strongly believes that relevant and timely threat information must be disseminated whenever possible. A number of sector representatives hold national security clearances that facilitate the sharing of classified threat information. In addition, the ESISAC facilitates communications between electricity sector participants, the Federal Government, and other critical infrastructures, and is a conduit for disseminating sensitive threat and incident information. A number of State and local authorities, with DHS support, have created Fusion Centers that combine relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities.

Asset owners and operators must rely on threat information from DHS and Federal, State, and local law enforcement organizations in order to assess the relative risk associated with a given asset. The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), which conducts integrated threat analysis for all CI/KR sectors, will work in partnership with owners and operators and other Federal, State and local government agencies to ensure that suitable threat information is made available. Furthermore, the same level of partnership must exist within all levels of Federal, State, and local law enforcement.

The following types of threat products provided by HITRAC are needed for the Energy Sector:

- **Common Threat Scenarios**, which present methods and tactics that could be employed in attacks against the U.S. infrastructure;
- **General Threat Environment Assessments**, which are sector-specific threat products that include known terrorist threat information and long-term strategic assessments and trend analyses of the evolving threats to the sector's critical infrastructure; and

- **Specific Threat Information**, which is critical infrastructure-specific information based on real-time intelligence, and that will drive short-term measures to mitigate risk.

In addition to these products, the Energy Sector further benefits from the continuation of:

- Periodic conference calls with asset owners and operators to relay recently reported suspicious activities near energy facilities and other pertinent unclassified threat-related information;
- Reports analyzing suspicious activities said to have occurred near energy facilities;
- Classified threat briefings for representatives of the energy industry. Various Federal agencies would use these briefings to inform industry representatives about general and specific threats associated with the Energy Sector, as well as the overall threat of terrorism to the Nation. Such briefings should include representatives of intelligence community members, as appropriate;
- Improved communications and increased participation with regional, State, and local joint terrorism task forces and organizations; and
- Interagency forums and workgroups, such as the Forum for Infrastructure Protection, Pacific Northwest Economic Region (PNWER), and other State and local information-sharing, emergency-planning, and exercise efforts that benefit the Energy Sector as well as other participating sectors.

These forums and materials provide insights to sector security partners regarding the overall threat to the energy industry. More specifically, they help energy facilities, local law enforcement, and others to be more aware of potential indicators of terrorist and/or criminal activity.

3.5 Assessing Vulnerabilities

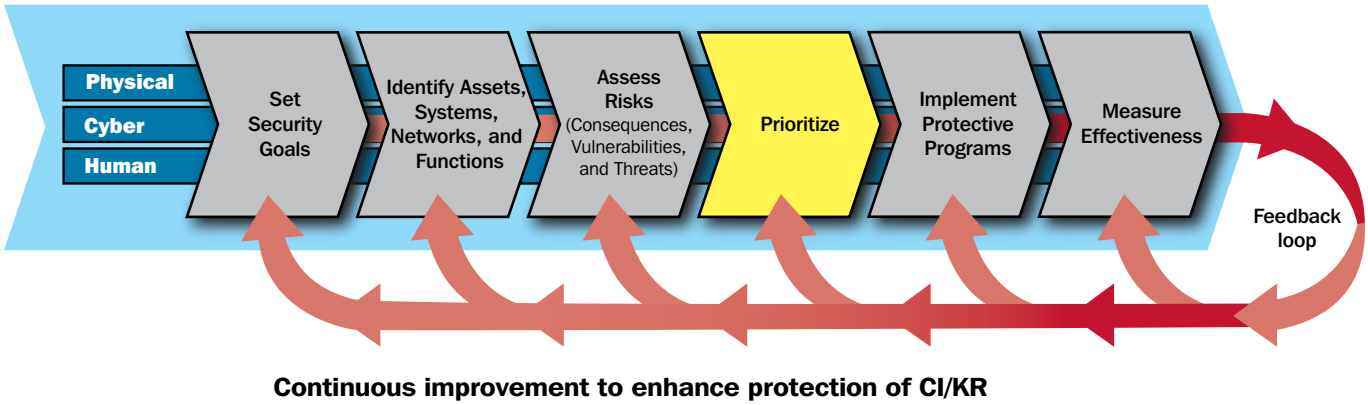
Vulnerabilities are the characteristics of an asset, system, or network's design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. Vulnerability assessments identify areas of weakness that could result in consequences of concern, taking into account intrinsic structural weaknesses, protective measures, resiliency, and redundancies.

Historically, the Energy Sector has been proactive in developing and applying vulnerability assessment methodologies tailored to its assets and systems. However, no single vulnerability tool or assessment methodology is universally applicable. Individual energy companies use assessment tools that are developed by professional and trade associations, Federal organizations, government laboratories, and private sector firms. The number of tools in use is large, and the vast majority of significant facilities in the Energy Sector have already undergone assessments using one or more of these tools.

The Energy Sector owners and operators have also participated in DHS/DOE-led site assistance visits. During these visits, DHS professionals and other subject-matter experts assist asset owner/operators in assessing and characterizing vulnerabilities at their critical infrastructure sites. These visits are designed to facilitate vulnerability identification and mitigation discussions between government and industry. They also help DHS identify vulnerabilities that are common to specific asset types, subsectors, and sectors. At the conclusion of a Site Assistance Visit, DHS representatives brief the asset owner/operator on identified vulnerabilities and protective measure options that are being used throughout the sector. The Site Assistance Visit team also authors a classified or unclassified report for the facility. The information learned at these site visits is used to develop Characteristics and Common Vulnerabilities Reports for different sectors and subsectors.

4. Prioritize Infrastructure

Figure 4-1: Prioritize



As explained in previous chapters, the Energy Sector is characterized by large networks as opposed to discrete assets. These networks are designed to operate with certain levels of reliability, even if portions of them (discrete components, or assets) are out of service.

The importance of many of the individual components in the network is highly variable, depending upon location, time of day, day of the week, month of the year, and many other variables. What might be a critical asset on a Monday morning in January may not be critical on a Saturday afternoon in May.

Owners and operators of Energy Sector assets and networks have screening processes to identify internal priorities related to business conditions and supply/network reliability to help them ensure continuity of operations. From a grid perspective, the Nation's oil and natural gas pipeline systems and electricity grid are designed and operated with built-in redundancy to ensure a certain degree of reliability and resiliency. Industry planning criteria assume a local grid area can be operated even if one asset is out of service. In addition, during unforeseen events, the industry provides mutual aid to assist in emergency response and prompt restoration[35] (chapter 5).

Regional planning groups for the oil and natural gas industry, and historically the NERC and regional reliability councils for the electricity industry, continuously evaluate network reliability. Their functions are well developed and understood, and the

[35] The effectiveness of mutual aid agreements can be significantly affected by the nature of an event. Mutual aid partners could also be impacted by an event, and a utility might have to go outside the region to obtain aid. It should also be noted that response and restoration may be affected by shortages in critical components, such as transformers and other high-voltage equipment, most of which have long lead times for replacement (12 to 24 months) and are foreign-produced.

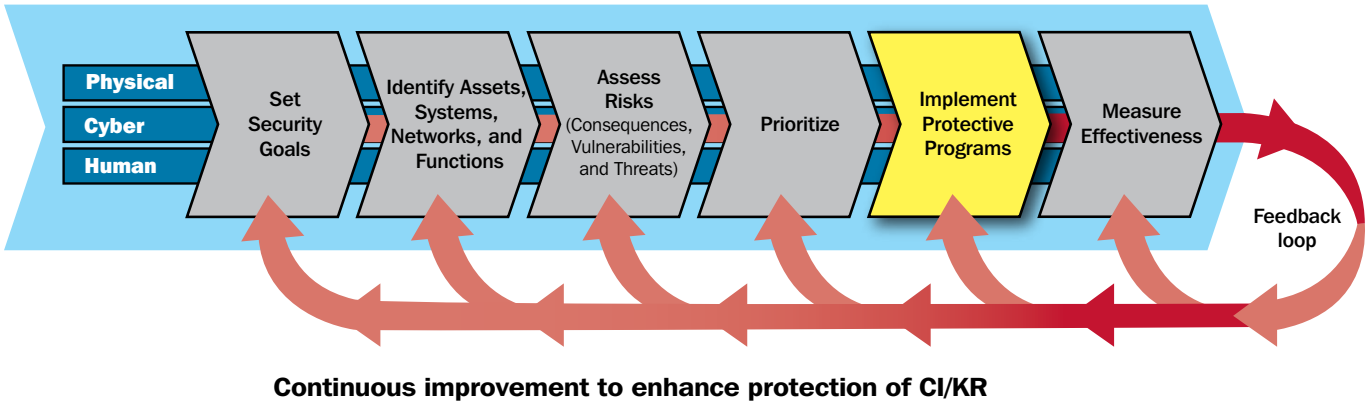
United States has among the most reliable electric and natural gas grids in the world. Further, energy industry groups have and continue to engage in exercises to plan for and ensure grid reliability. With implementation of FERC's electricity reliability authorities under the Energy Policy Act of 2005 (EPAct 2005), the Federal role in electricity reliability is greatly enhanced.

The Energy Sector has well-developed protocols, organizations, and systems for ensuring the reliability of the energy network. The importance of sector assets is impacted by changing threats and continually changing consequences. Prioritization in the Energy Sector is dynamic—it changes constantly and goes on continuously. Static prioritization of Energy Sector assets could lead to critical decisionmaking based on outdated or erroneous asset information in efforts to direct scarce resources to those assets, systems, and networks that may be the most critical at any point in time. DOE works with DHS to identify gaps in existing energy information and to identify publicly available databases or sources that could provide data to support DHS efforts to prioritize assets.

Some DHS, DOE, and other government programs need to allocate resources based on their prioritization (e.g., DHS's BZPP), Site Assistance Visits and comprehensive reviews, as well as State and local initiatives). These programs supplement and support industry efforts. State and local efforts under the NIPP will be based on some measure of the relative importance, risk consequence, and vulnerability of the critical infrastructures within their jurisdictions. This will require that they work with the Energy Sectors in their jurisdictions so as to understand the importance of critical facilities. In addition, they will need to address policy, regulatory, or other barriers to undertake needed measures and to allow for recovery of prudently incurred costs for those utilities subject to rate regulation. In addition DHS is providing funding to State and local entities based on risk assessments of critical infrastructures. The National Asset Database (NADB) is also organized by criteria that may not fully capture the relative importance of energy infrastructure from a systems perspective. These issues will need to be addressed as this planning process evolves.

5. Develop and Implement Protective Programs

Figure 5-1: Implement Protective Programs



5.1 Overview of Sector Protective Programs

DOE will continue to work in partnership with Energy Sector security partners to evaluate and support existing protective programs and to develop and support new programs that effectively reduce the vulnerability of critical energy assets. The overall strategy will focus on efforts that support the sector's goals to ensure continuity of energy services and business through reliable information sharing, effective physical and cyber security protection, and coordinated response capabilities.

The cornerstone of the overall strategy is partnership with all key stakeholders in the public and private sectors. This approach will continue to take full advantage of the extensive experience and expertise of sector partners and will ensure that repercussions of planned activities are carefully considered. This chapter outlines the methods that Energy Sector partners will use to assess, select, and implement cost-effective infrastructure protective programs and highlights some of the existing cooperative efforts within the Energy Sector.

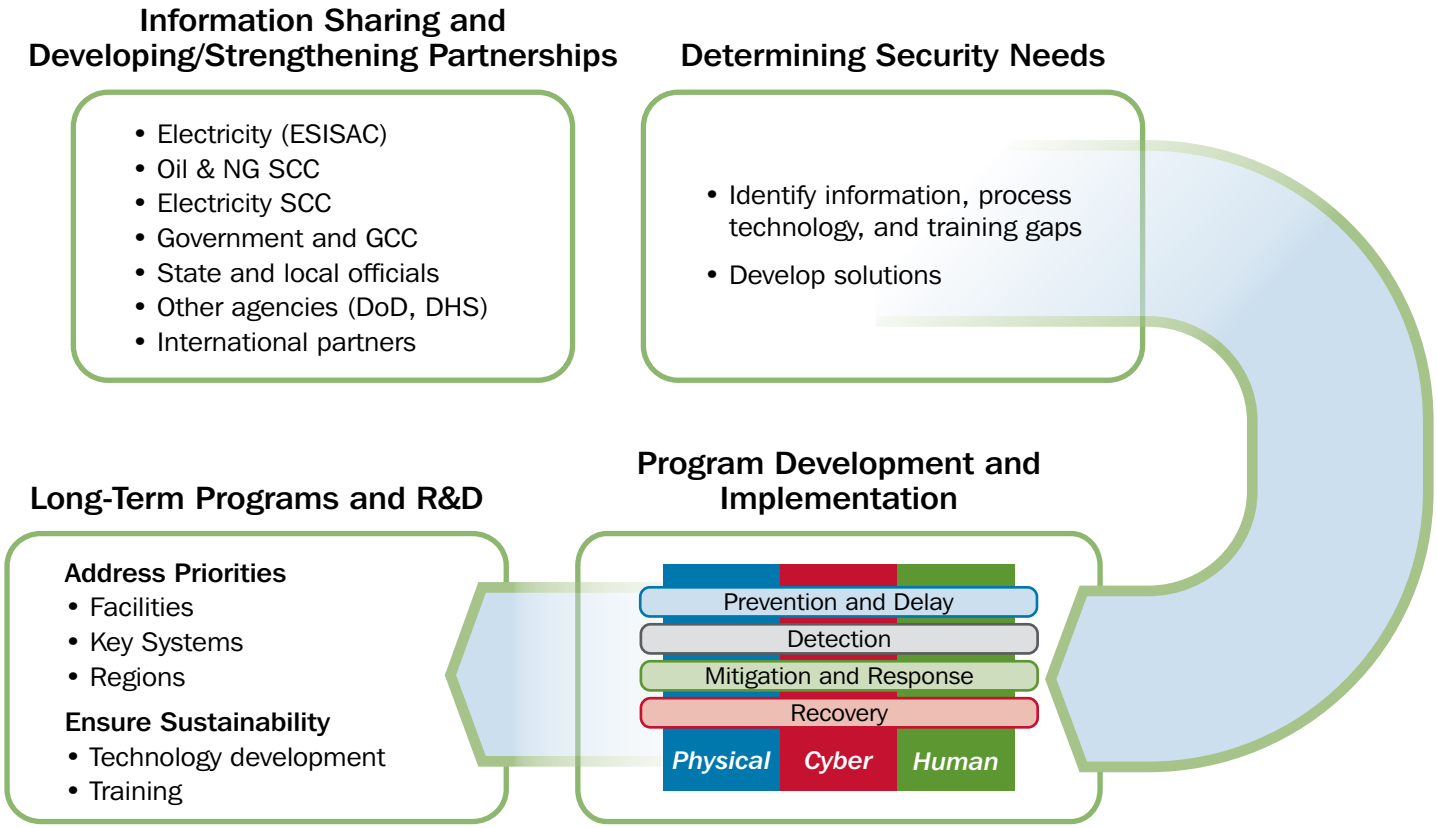
5.2 Process for Evaluating, Prioritizing Needs, and Implementing Programs

The process for developing and implementing effective protective measures has three phases: determining needs, developing programs, and finding long-term solutions (figure 5-2). The first phase will build on information sharing and partnerships to determine security needs. The second phase, program development and implementation, will draw from effective practices already in use by industry and from national laboratory efforts. The last phase will address R&D needs (discussed in chapter 7)

and identify long-term technological solutions for protecting physical assets, energy control systems, and related cyber systems. Some activities in different phases may proceed simultaneously, where feasible, to expedite improvements in CIP.

Throughout the process, DOE will continue to work with security partners within the framework of the Energy Sector's goals who support its vision of a "robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government."

Figure 5-2: Evaluating and Prioritizing Needs, and Implementing Programs



5.2.1 Enhanced Information Sharing and Needs Assessment

During the needs assessment phase, DOE will work closely with the industry and GCCs and its other security partners to:

- Enhance current information-sharing practices and programs;
- Identify information gaps/needs;
- Augment current efforts to develop protection guidelines and programs;
- Develop an understanding of roles and responsibilities in strengthening protection of energy assets;
- Support owners and operators and their representatives in evaluating existing practices and guidelines for reducing physical and cyber vulnerabilities;

- Update and improve existing protective and resiliency programs and methods as warranted;
- Conduct training and exercises with Federal, State, and local officials and industry representatives that test and identify gaps in current approaches to security, preparedness, response, and energy assurance issues, and recommend programs to address any identified gaps; and
- Conduct site assistance visits to energy asset owners and operators.

5.2.2 Developing and Implementing Focused Programs

Development of resiliency and protective programs will be done in close consultation with key industry and State officials and in partnership with DHS and other appropriate Federal Government agencies. Programs will draw from effective practices already in use by industry and from national laboratory efforts. Specific programs will be designed to account for the significant interdependencies between energy and the other infrastructures. Energy Sector security partners will evaluate potential programs developed for an asset or group of assets.

Establishing roles and responsibilities for implementation of new resiliency and protective measures and programs will present both a challenge and an opportunity. DOE will continue to work with DHS and other agencies as well as industry owners and operators to examine policy and regulatory issues surrounding establishment of such programs.

Finally, comprehensive programs that address the vulnerabilities of high-priority assets within the infrastructure will be implemented or enhanced, along with complementary training and exercise programs. Roles and responsibilities for developing, implementing, and maintaining resiliency and protective programs will be clearly delineated among DOE, DHS, other Federal agencies (DOT and TSA, for example, regarding pipelines), sector asset owners, and State, local, and tribal officials.

5.3 Program Development and Sector Goals

Extensive programs are already in place to support and protect the Nation's energy resources and cyber assets. Review of these existing security programs and development of new ones will be done within the framework of the sector's goals, which as previously noted, can be grouped into four main categories: information sharing and communication, physical and cyber protection, coordination and planning, and public confidence.

5.3.1 Information Sharing and Communication

Goal: Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector security partners.

Both industry and government need credible, timely, actionable threat information to ensure that the most appropriate security investments, programs, and decisions are made to protect sector assets. Information on vulnerabilities, threats, and consequences is, by nature, sensitive. Unless both public and private sector security partners trust that shared information will be strictly protected and used only for agreed-upon purposes, the costs of sharing sensitive information may be seen to outweigh the benefits, and the partnership will fail. Trusted relationships between the decisionmakers who implement risk management programs will provide the most effective foundation for coordinated response functions and effective information-sharing programs.

High on the list of challenges is the need to develop new methods or to better explain existing methods that are acceptable to all stakeholders for collecting, protecting, and, as necessary, sharing sensitive data on the vulnerabilities of energy assets and the protective programs to address them. Industry will be understandably cautious in providing information needed for vulnerabil-

ity assessments and disclosing the results of assessments it has conducted, and may be equally cautious about providing specifics on ongoing and planned protective programs.

Responding to such industry concerns, DOE will continue to work closely with industry, States, DHS, FERC, and other agencies to develop suitable information exchange policies, regulations, and procedures to protect all industry information against inappropriate disclosure. DOE will also continue to work with the PCII Office within DHS's OIP to apply provisions of the Critical Infrastructure Information Act of 2002 (CII Act) and the implementing regulations at 6 CFR Part 29 to critical infrastructure information that is not customarily in the public domain and is voluntarily submitted to DHS.

5.3.1.1 Industry Programs

Both the electricity and oil and natural gas subsectors have made extensive efforts to share security information. In the electricity industry, NERC operates ESISAC, which gathers, disseminates, and interprets security-related information (Figure 5-3). It facilitates communication among electricity industry participants, Federal agencies, and other critical infrastructures, and helps electricity sector participants take protective actions. In addition, a procedure for reporting suspected or real security incidents is in place along with a NERC standard that requires entities to report physical sabotage. The cyber standards adopted by the electricity industry also require reporting.

In the oil and natural gas industry, AGA, the National Petrochemical and Refiners Association (NPRA), API, as well as other oil and natural gas industry groups, have held numerous workshops and forums to discuss and share security information. The industry has also worked closely with DHS, DOT, and DOE to develop security guidelines and has continued to conduct regional planning studies to determine the impact of major pipeline system outages.

Figure 5-3: ESISAC Functions

- Receives incident data from private and public entities.
- Assists DOE, FERC, and DHS in analyzing event data to determine threat vulnerabilities and trends, as well as interdependencies with other critical infrastructures.
- Facilitates analysis of incident data and prepares information.
- Disseminates threat alerts, warnings, advisories, notices, and vulnerability assessments.
- Maintains a close operating liaison with other private and public government infrastructure information-sharing and analysis centers.
- Develops and maintains an awareness of private and government infrastructure interdependencies.
- Maintains a secure Internet site to facilitate messaging among participants.
- Participates in government infrastructure exercises.
- Conducts outreach.

5.3.1.2 Government Programs

In a joint effort, DHS has partnered with the Energy Sector SCCs to develop HSIN, an Internet-based communications system[36] that enhances reporting and information sharing and allows industry participants to communicate securely with each other, with other industry sectors, and with government agencies (figure 5-4). The ONG SCC signed an HSIN Memorandum of Understanding (MOU) with DHS in May 2006, and the ESCC is working on a pilot for HSIN. DOE has also developed the ISERnet, a restricted-access communications network for key energy industry and State personnel to exchange information with the Department during energy emergencies. The site provides threat awareness and relevant security analyses and presentations.

Public Safety and Emergency Preparedness Canada (PSEPC) and DHS exchange government information via HSIN. PSEPC and the Canadian Electricity Association regularly exchange information via voice and electronic media. PSEPC and NERC exchange information via ESISAC. In addition, DHS and PSEPC have the necessary mechanisms in place to facilitate sharing of electricity sector threat and vulnerability information between the Canadian and U.S. governments.

[36] HSIN is a secure, Internet-based system of integrated communication networks designed to facilitate information sharing between DHS and other Federal, State, county, local, tribal, and private sector commercial and other nongovernmental organizations involved in identifying and preventing terrorism, as well as in undertaking incident management activities.

DHS/Office of Infrastructure Protection (OIP) provides briefings and information for cleared members of the Energy Sector to enable attendees to assess risks facing the industry.

The EEAC system is a cooperative effort among associations representing States, local governments, and DOE/Office of Electricity Delivery and Energy Reliability's ISER. EEAC provides energy security information, including daily news summaries, emergency situation reports, lessons learned from other States, links to outage and curtailment information, and the ability to email messages to colleagues in other jurisdictions. In an energy supply disruption or emergency, DOE relies on these contacts to provide an up-to-date assessment of energy markets in the affected States. They serve as the link between the State, industry, and DOE.

Figure 5-4: Oil and Natural Gas Homeland Security Information Network Functions

- Serves as a mechanism for gathering and disseminating private sector information as well as information from the Federal Government.
- Becomes a clearinghouse of information within and among various sectors of the energy industry.
- Becomes a repository of historical data to be used by its members.

5.3.2 Physical and Cyber Security

Goal: Use sound risk management principles to implement physical and cyber protective measures that enhance preparedness, security, and resiliency.

DOE will work with DHS and other Energy Sector partners to assure that current and potential threats are conveyed on a real-time basis to owners and operators. The need for increased and continuous vigilance is clear.

The Energy Sector has a long history of understanding and mitigating risk. The industry has rapidly responded to the increased need for enterprise-level security efforts and business continuity plans, and will continue to assess the security vulnerabilities of single-point assets such as refineries, storage terminals, and power plants, as well as networked features such as pipelines, transmission lines, and cyber systems.

Significant time and resources will be needed to address identified vulnerabilities of high-priority energy assets. Once challenges are addressed, the Energy Sector will draw on its experience with data collection and interpretation to establish processes and methods for collection, protection, and use of data associated with resiliency and protective programs.

It is also necessary to work with industry to develop a sound business case supporting resiliency and protective programs. Once a business case is developed, the challenge remains to make the necessary supporting data readily available to government and business decisionmakers who must allocate funds to a specific asset or system to mitigate a threat that could be directed against an entire industry or sector.

5.3.2.1 Industry Programs

Today's developing "information age" technology has intensified the importance of CIP, in which cyber security has become as critical as physical security to protecting energy CI/KR. The Energy Sector has rapidly responded to the increasing need for enterprise-level physical and cyber security efforts and business continuity plans. Voluntarily conducted vulnerability assessments have not only improved sector security but have also demonstrated industry commitment to a secure and resilient Energy Sector. Many asset owners and operators conduct self-assessments or contract with third parties to perform energy vulnerability assessments and implement protective programs at their facilities.

Electricity

NERC has developed Cyber Security Standards CIP-002 through 009,[37] which have been filed with FERC for approval and address the following requirements:

- Data and information classification according to confidentiality;
- Identification and protection of cyber assets related to reliable operation of the bulk electric systems; and
- Process control, SCADA, and incident reporting.

NERC's CIPC has issued a summary of several electric power vulnerability assessment methodologies, including a variation of DOE's Vulnerability and Risk Analysis Program methodology, in a suite of potential vulnerability assessment tools that electric power companies should consider using.

Oil and Natural Gas

The oil and natural gas subsector has identified the following priorities:

- Assess security vulnerabilities at single-point assets such as refineries, storage terminals, and other buildings, as well as networked features such as pipelines and cyber systems; and
- Work toward resilient and secure cyber networks and SCADA systems to detect and respond to cyber attacks.

The AGA, the Interstate Natural Gas Association of America (INGAA), and APGA worked together to develop and release *Security Guidelines: Natural Gas Industry, Transmission and Distribution*. These guidelines provide an approach for vulnerability assessment, a critical facility definition, detection/deterrent methods, response and recovery guidance, cyber security information, and relevant operational standards. The industry security guidelines incorporate a risk-based approach for natural gas companies to consider when identifying critical facilities and determining appropriate actions, and are based on the DHS Homeland Security Advisory System (HSAS). The TSA, along with the PHMSA, is currently conducting onsite reviews based on these guidelines.

5.3.2.2 Government Programs

PHMSA, in cooperation with energy and pipeline trade associations and State pipeline safety programs, has issued a security guidance information circular that defines critical pipeline facilities, identifies appropriate countermeasures for protecting them, and explains how PHMSA plans to verify that operators have taken appropriate action to implement satisfactory security procedures and plans.

Many State public utility commission and other State agencies are responsible for administering the Federal/State Pipeline Safety Programs as established by 49 U.S.C. Chapter 601. Although pipeline security falls under the Transportation SSP, many States have safety regulatory responsibilities for pipelines under this program since they are a key aspect of the energy infrastructure.

States and local government also have responsibilities for working with the private sector on the physical and cyber security of energy facilities. Public utility commissions are responsible for assuring an adequate and reliable supply of electricity, natural gas, and in some cases, petroleum. They must address cost recovery of utility investments that protect and enhance the resiliency of the energy infrastructure. Public utility commissions along with State energy offices also respond to energy supply disruptions and develop, maintain, and exercise contingency plans. Cyber security has been a concern of the commissions since the late 1990s, when questions arose about how reaching the year 2000 might affect computer and control systems (Y2K). Some States have also supported cyber security efforts by working with the InfraGard program.

State homeland security agencies also are responsible for ensuring that a State's critical energy infrastructures are protected as part of the State homeland security strategy. This includes working with DHS on comprehensive security reviews at key energy

[37] www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

facilities, and working with local governments to provide BZPPs around the perimeters of critical infrastructures. In some cases local governments also own and operate municipal electric utilities and have direct responsibility for undertaking risk and vulnerability assessments and implementing protective measures.

5.3.2.3 International Programs

The U.S. and Canadian governments have signed the Canada-United States CIP Framework for Cooperation, which recognizes their shared commitment to a secure and robust critical infrastructure. The framework includes energy as well as transportation and other sector infrastructure and is evidence of the mutual commitment by each country to work for the protection of shared critical infrastructure.

The United States and Mexico also work together under a U.S.-Mexico Critical Infrastructure Framework for Cooperation. A CIP Bilateral Steering Committee oversees the six working groups that implement the framework in the areas of energy, transportation, public health, telecommunications, food and agriculture, and water and dams.

Trilaterally, an Ad Hoc CIP Forum under the North American Energy Working Group (NAEWG) promotes a more fully integrated energy market in North America. NAEWG was established in 2001 by the U.S., Canadian, and Mexican energy departments.

5.3.3 Coordination and Planning

Goal: Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.

Goal: Clearly define CIP roles and responsibilities among all Federal, State, local, and private sector security partners.

Goal: Understand key sector interdependencies and cooperate with other sectors to address them, and incorporate that knowledge in planning and operations.

Coordination and cooperation are key to planning and executing security programs and response and recovery activities. Security programs and emergency response planning will be most effective when stakeholders clearly understand their respective roles and responsibilities and plan to integrate their independently executed roles to achieve a common set of infrastructure protection outcomes.

The Energy Sector depends on other sectors to help provide its services, and it provides energy services upon which numerous other sectors depend. Interdependencies also exist within the sector itself. Comprehensively understanding such interdependencies will enable the sector to mitigate any potential vulnerability and help ensure that the Nation's economy can continue to deliver goods and services during extraordinary events. DOE will work with sector security partners to help identify program gaps improve the effectiveness of the Energy Sector security programs.

5.3.3.1 Coordination With Industry

In the electricity subsector, collaboration between NERC and DOE allows for industry-government cooperation and coordination on CIP efforts in the physical and cyber security areas. NERC's CIPC coordinates several working groups and task forces that address specific issues related to NERC's security initiatives and protection of the electric system. CIPC is composed of industry experts in the areas of cyber security, physical security, and operational security. Both DOE and DHS also participate in CIPC so it can serve as a mechanism within the electricity sector for collaboration between industry and government to identify and close gaps in sector-wide efforts to meet the sector's goals.

The oil and natural gas industries also have longstanding partnership with all levels of government in efforts to coordinate infrastructure protection efforts. As with the electricity sector, the ONG sector, working with DOE, DHS, and DOT, has created its own security guidelines and security vulnerability assessment methodology. The ONG SCC and the CIPAC also provide a mechanism for the industry to improve collaboration on protective programs among themselves and with DOE, the Energy GCC, individual Federal agencies, and State government energy associations.

5.3.3.2 Coordination With Federal Government Agencies

DOE and the sector security partners will coordinate with other Federal agencies that have energy-related response and security responsibilities and energy-related programs. DOE will continue to support effective practices and partner, where practical, with these agencies in implementing protective programs. The responsibilities of various government agencies under the National Response Plan are an important element of intra-governmental cooperation during an energy emergency or other incident of national significance. During disruptions, DOE staff and emergency response support personnel work in conjunction with personnel from FEMA, DHS, EPA, DOT, State and local government, utilities, and others as they perform DOE's Emergency Support Function 12 (ESF-12) responsibilities. DOE has also partnered with several Federal agencies (including FERC), State regulators, and industry to assess the implications of a loss of natural gas supply to certain regions of the country.

5.3.3.3 Coordination With States and Localities

State and local governments have a unique role in energy assurance because they represent the front lines of protection and the face of public services to citizens during an emergency. As the SSA for the energy infrastructure, DOE has engaged the State and local energy leaders and the organizations that represent them in an effort to identify their energy assurance needs and to implement programs directed at improving the reliability and safety of their energy infrastructure.

NASEO, in collaboration with NARUC, has produced Energy Assurance Guidelines that outline the States' overall role in energy assurance, including operating within the Federal emergency support function structure, organizing and building response mechanisms, coordinating with stakeholders, planning response strategies, profiling energy use and vulnerability, and identifying fuel-related response measures. NARUC and NASEO have worked with DOE to conduct multi-State and regional exercises and training sessions on energy emergency preparedness, response, and key CIP issues. NASEO, with DOE support, has also provided direct technical assistance to States to update their energy emergency plans.

DOE will continue to work with State and local governments to identify gaps in meeting sector goals, improve existing State-focused programs, and implement new programs to eliminate gaps and identified vulnerabilities. Because of State responsibilities for public utilities that provide a direct service to their citizens, States are particularly concerned with programs related to protection of, interdependencies among, and sharing of information with other critical sectors (see figure 5-5, "Public Utility Commissions"). Public utility commissions also support emergency management and response activities during emergencies or disasters that affect utility facilities, systems, and services.

Figure 5-5: Public Utility Commissions

Public utility commissions provide an example of a State entity with responsibility for electricity, gas, and telecommunications infrastructures and, in some cases, water, wastewater/sewage, and certain aspects of transportation. As such, public utility commissions are uniquely positioned to deal with the recovery of investments made for CIP in these areas. Furthermore, public utility commissions historically have been concerned with the adequacy and reliability of these services, and have facilitated investments made by these industries to ensure that they are resilient and reliable.

For example, public utility commissions work together to address issues of mutual concern based on the interdependencies between the water, telecommunications, and energy infrastructures (in the context of preparedness for, and response to, events impacting critical infrastructure) by:

- **Creating networks among utility regulators and other Federal, State, local, and private sector entities to address cross-sector issues;**
- **Exploring and recommending solutions for information disclosure issues (especially protecting sensitive security information from public disclosure while ensuring that all critical stakeholders have access to essential information);**
- **Exploring and recommending solutions to cost-recovery issues associated with key water, gas, telecommunications, and energy infrastructures; and**
- **Identifying and prioritizing issues, researching best practices, and disseminating information to Federal and State partners and affiliates.**

NIPP, June 30, 2006, p. 26.

5.3.3.4 Regional Coordination

It is important for all Energy Sector security partners to coordinate on the national level to ensure synergy of efforts and efficiencies. Regional coordination, however, may be even more important, especially regarding response to actual events. In the electricity sector, cooperation between utilities on a regional basis has been taking place for many years. There are eight Regional Mutual Assistance Groups at present: Great Lakes, Mid-Atlantic, Midwest, New York, Southeastern Electric Exchange, Texas, Western Region, and Wisconsin. Figure 5-6, "Southeastern Electric Exchange Mutual Assistance Group", provides an example of how such regional cooperation can work.

Similarly, PNWER provides an example of regional coordination between public and private partnerships. The organization includes legislators, State governments, and businesses in five States and three Canadian provinces. PNWER sponsors interdependency exercises and has developed an action plan outlining several physical and cyber CI/KR regional protection projects. PNWER also participates in Northwest Warning, Alert, Response Network (NW-WARN), a DHS alert and response network pilot project.

Figure 5-6: Southeastern Electric Exchange Mutual Assistance Group

The Southeastern Electric Exchange has had a formal working mutual aid group since the 1950s. The group has established written guidelines for requesting and providing emergency assistance that are continuously improved and refined. The Edison Electric Institute (EEI) has created a "Joint Mobilization" process that includes establishing a procedure for initiating "Mutual Assistance Conference Calls." This procedure allows a company in need of assistance to contact all members with one phone call. After each call, all members receive summary notes and a "Resource Summary Sheet," which details the resources needed and available, including companies and contract personnel. Most commonly requested and identified resources include distribution linemen, transmission linemen, vegetation management personnel, and damage assessment personnel.

At least five of the other mutual assistance groups have adopted conference call procedures similar to Southeastern Electric Exchange's.

5.3.3.5 International Coordination

The U.S. Energy Sector relies on energy and technology imported from other countries. Therefore, it is critical that the United States work closely with these countries to reduce physical and cyber vulnerabilities within their own energy sectors, as these vulnerabilities could affect the U.S. energy infrastructure. DOE, in conjunction with DHS, DOS, and other Federal agencies, cooperates in bilateral and multilateral forums with other countries.

The United States and Canada have a well-established history of collaboration and cooperation on electricity reliability, primarily through NERC. EPAct 2005 requires implementation of mandatory electricity reliability standards in the United States. These reliability standards will be paralleled by implementation in Canada. The United States and Canada have developed an even closer working relationship through the joint task force established to investigate the causes of the largest power blackout in North American history, in August 2003, and to develop recommendations to reduce the possibility and scope of future outages. A bilateral group composed of senior staff members from FERC, DOE, and NRCan has ongoing responsibility for monitoring and implementing the recommendations of the Blackout Report, which was published in October 2006. Twelve of the recommendations from this report address enhancing the physical and cyber security of the North American Bulk Power Systems.

Pipeline interconnections between the United States and Canada and between the United States and Mexico move considerable volumes of oil and gas between the countries. This also requires coordination to assure that protective measures across borders assure adequate risk reduction across the full length of these systems.

5.3.4 Public Confidence

Goal: Strengthen partner and public confidence in the sector's ability to manage risk and implement effective security, reliability, and recovery efforts.

Industry and government officials will work to communicate to Congress, regulators, and the general public that the industry's public-private partnership is working effectively to ensure sector security. Agencies and industry associations have publicized their efforts. DOE will continue to work through the SCC and GCC members to support additional ways to enhance public confidence, including education and communication programs.

5.4 Program Performance, Gaps, and Challenges

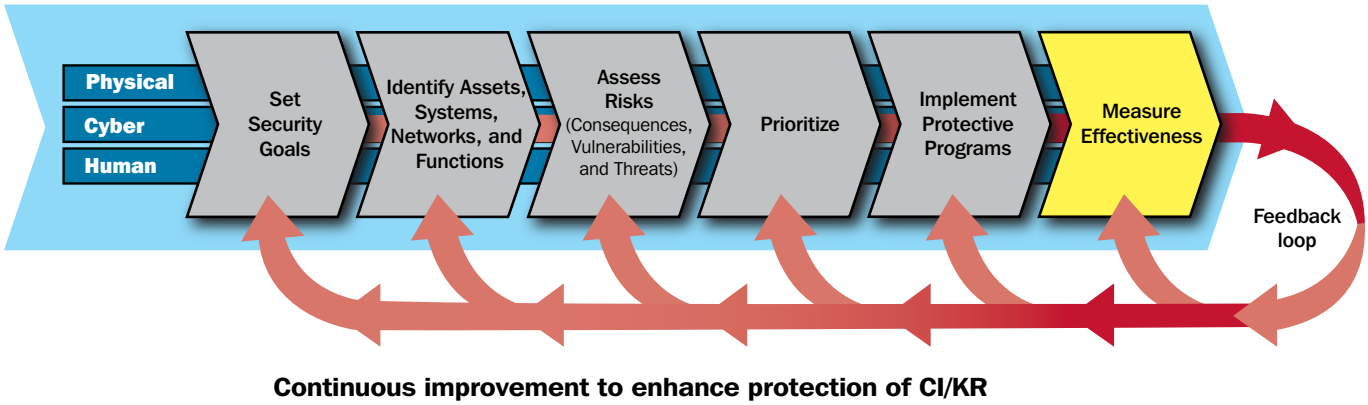
Table 5.1 lists some of the recommendations from energy industry symposia held to discuss lessons learned. Many of the industry recommendations present challenges to be addressed or indicate a need for education on response procedures and legal restrictions. Chapter 6 addresses metrics that may be used to evaluate program performance.

Table 5.1: Energy Sector Gaps and Recommendations

Transportation and Access to Disaster Areas
• Develop personnel and vehicle identification to control access to disaster areas to facilitate restoration efforts. • Provide assistance for travel within and to and from disaster areas in clearing roads and helping local public safety officials manage traffic flow. • Facilitate the availability of fuel supplies to be used for restoration equipment and crew transportation.
Health and Safety of Utility Crews Deployed in Disaster Areas
• Facilitate the health and safety of utility crews in disaster areas. • Educate responding government agencies on the need to facilitate delivery of supplies and equipment needed by crews and other critical infrastructure workers. • Advise companies of requirements for inoculations and other preventive health care considerations before crews are sent to a disaster area.
Communications
• Collect and disseminate appropriate outage and restoration information via existing emergency communication channels such as NERC, State emergency agencies, DOE 417 reports, or trade associations, as well as the Energy Emergency Assurance Coordinator (EEAC) and the ISERnet secure Web sites. • Coordinate and prioritize the restoration process between government and energy companies. • Provide priority status on cellular and satellite communication systems to all key Energy Sector partners.
Pre-Event Coordination
• Develop mutual contact information for key personnel and protocols for utilizing it. • Plan and coordinate disaster-planning drills on State and regional bases. • Compile a document of all State and Federal government programs and plans that may provide benefit to companies and crews responding to disasters.

6. Measure Progress

Figure 6-1: Measure Effectiveness



DOE will continue to work with Energy Sector partners to measure progress toward achieving the critical infrastructure protection goals outlined in chapter 1. An effective performance measurement system identifies appropriate metrics for measuring progress, collects relevant data on each metric, and uses that data to improve performance and provide accountability. DOE and Energy Sector partners are in the process of identifying an initial set of metrics that are specific to the Energy Sector to supplement the DHS metrics that are common across all CIP sectors. Once metrics have been identified and agreed upon, initial assessments will be conducted to provide baseline information on each metric.

The Energy Sector recognizes that the measurement process itself can expose sensitive information about the vulnerability and protective capability of the energy infrastructure. DOE and Energy Sector partners will work with the PCII Program Office within DHS OIP to apply the provisions of the CII Act, and the implementing regulations contained in 6 CFR Part 29, to critical infrastructure information that is not customarily in the public domain and is voluntarily submitted to DHS. DOE will not request or hold sensitive energy-related critical infrastructure information (beyond what it currently holds or collects) unless and until it is able to protect this information, and will use this information only for national infrastructure protection purposes.

6.1 CI/KR Performance Measurement

6.1.1 Metrics

DHS plans to use two classes of metrics to track performance: core metrics and sector-specific metrics. Core metrics are intended by DHS to be common across all sectors. Sector-specific metrics are developed by sector security partners and are tailored to the individual sector.

6.1.1.1 Core CIP Metrics

The core metrics are a set of descriptive, process, and outcome metrics that measure progress made by and across all CI/KR sectors in implementing the NIPP Risk Management Framework. These metrics are still being developed by DHS in conjunction with the SSAs and other security partners. When these core metrics are finalized, DOE will continue to work with the energy SCCs and the energy GCC to identify the most effective and cost-efficient way to collect responses to submit on behalf of the sector. Core metrics will be assessed as appropriate, consistent with DHS requirements.

6.1.1.2 Energy Sector Metrics

DOE and Energy Sector security partners will develop an initial set of sector-specific CIP metrics through a collaborative process involving the energy SCCs and GCC. Meantime, qualitative and quantitative measures to track progress toward the sector goals are currently being developed. They will be periodically reviewed by the SCCs and GCC and modified as necessary to meet the evolving challenges facing the Energy Sector. It is expected that, over time, some of these qualitative measures will be replaced with quantitative indicators as well as output and outcome metrics.[38] These qualitative measures and energy-specific metrics will be supplemented with anecdotal information on how well the sector is performing.

6.1.2 Information Collection and Verification

DOE and its Energy Sector security partners will identify sources and methods for collecting and sharing data on the Energy Sector CIP metrics once they are identified.

6.1.3 Reporting

Data relating to the sector-specific metrics and core metrics will be reported annually to DHS by DOE. All data will be reported at a summary level and will be suppressed if they could reveal information about an individual company or asset.

6.2 Implementation Actions

Energy sector security partners have identified actions to be completed as the Energy SSP is implemented over the next few years. These actions represent the major actions that DOE and some members of the sector will undertake to maintain a robust, resilient energy infrastructure. Successful completion of these actions depends on the availability of public and private resources.

DOE, as the SSA for energy, will work with the energy SCCs and GCC in cooperation and coordination with all energy security partners under CIPAC.

Efforts will build on existing work in government agencies as well as private sector partners.

[38] Output metrics measure whether specific activities were performed as planned to track progression of a task or report on the output of a process (such as inventorying assets). Outcome metrics track progress toward a strategic goal by the beneficial results rather than by the level of activity. See the NIPP Base Plan, p. 49.

6.3 Challenges and Continuous Improvement

Data on the sector-specific and core metrics will be examined to determine whether additional actions could be taken that might improve the security and resilience of the Energy Sector. For example, if only a small portion of the Energy Sector is participating in HSIN, then sector security partners could be asked why they are not involved. Appropriate corrective actions would depend on the reasons for not participating, but may range from disseminating additional information about the benefits of participating to notifying DHS of particular problems with the network.

There are numerous challenges in using data for continuous improvement. First, data collection is costly and time-consuming. Second, sector security partners participate on a voluntary basis. Creative approaches may be needed to encourage and ensure participation. Third, some of the data that could be collected are sensitive. Some partners may be unwilling or unable to provide some types of information. Despite challenges, the Energy Sector will work to implement continuous improvement principles.

7. CI/KR Protection R&D

7.1 Overview of Sector R&D

R&D is a key source of innovation and productivity for the Energy Sector. The equipment and systems used to extract, refine, transport, generate, and deliver energy are among the most technologically sophisticated of any economic sector. The high levels of reliability and productivity achieved by our Nation's Energy Sector are largely a result of significant private and public capital investments made in new physical and cyber technologies.

Energy owners and operators have worked with government, national laboratories, universities, industry organizations, and other key stakeholders to drive technological innovation throughout the Energy Sector. In 2004, combined public- and private-sector spending on all energy R&D totaled roughly $4.5 billion, with industry contributing roughly one-quarter of that total.[39]

Improved infrastructure security and resiliency have become increasingly significant objectives of the Energy Sector's comprehensive technology R&D portfolio, as functionality and productivity are now coupled more closely with protective measures. The Energy Sector is composed of many different elements, each associated with different types of assets, business conditions, and risk profiles that define their distinctive and diverse R&D priorities. Companies work closely with their vendors, technology developers, customers, and research institutions to plan and manage R&D activities to meet their particular operating and security needs.

The Energy Sector's commitment to reliable energy services and a robust, resilient infrastructure depends on effective physical and cyber security protection. In the near term, many companies will enhance their protective posture by adopting existing technologies, effective practices, and low-cost retrofits. The current energy infrastructure represents a massive capital investment that cannot be easily replaced even if new technologies become available. As energy companies and utilities expand their physical plants and replace older capital stock, new technologies that incorporate enhanced security features may be adopted.

Federal R&D investments exist in many government agencies and are coordinated with those of the private sector as part of an effective and robust national R&D strategy. DOE works with DHS and other funding agencies to highlight sector R&D needs and to help identify priorities in cooperation with sector security partners. In particular, Federal R&D seeks to fill gaps and stimulate private investment, particularly where market forces alone are insufficient to attract adequate private R&D funding. Leveraging public and private R&D investment in collaborative projects of mutual benefit is a central principle in the Federal energy R&D strategy for CIP.

As the Energy Sector lead, DOE has a long history of collaborating with Energy Sector partners to develop new technologies. Since September 11, 2001, DOE, DHS, and other Federal agencies have collaborated on new technologies that will improve

[39] Daniel M. Kammen, Gregory F. Nemet. "Real Numbers: Reversing the Incredible Shrinking Energy R&D Budget," *Issues in Science Technology*, Volume 84, September 2005.

protection of energy assets. The Energy Sector and Federal Government are using the Sector Partnership Model to enhance this collaboration.

HSPD-7 requires development of an annual National Critical Infrastructure Protection R&D Plan. This plan, developed jointly by the DHS Science and Technology Directorate and the White House Office of Science and Technology Policy, addresses common issues faced by various sector security partners and ensures a coordinated R&D program that will yield the greatest value across all sectors. The energy SCCs and GCC will provide input to this plan and use it to help guide R&D planning efforts.

7.2 Energy Sector R&D Requirements

Energy sector stakeholders have become increasingly concerned about the security of the energy infrastructure. Since the 1990s, various groups such as the President's Commission on Critical Infrastructure Protection, NERC, and the National Petroleum Council have conducted numerous studies on the vulnerability and reliability of the Nation's energy infrastructure. Since September 11, 2001, additional studies, such as those conducted by the National Research Council[40] and RAND Corporation,[41] have examined the vulnerabilities and R&D needs of the Energy Sector in the new threat environment. In total, more than 100 studies of the energy infrastructure have been completed.

While these studies contain a variety of R&D recommendations, many were compiled by the research communities with little input from the private sector. The energy industry has a keen understanding of system operations and the potential consequences of critical failures, and shares responsibility for advancing R&D to make energy assets more secure. Government has also become increasingly aware of the need to stimulate security improvements in a competitive energy market that may inhibit private investment in security R&D. Consequently, industry and government are now actively working together to coordinate technology development through R&D roadmaps, government program reviews, and professional conferences and workshops to leverage limited resources for maximum gain.

Cyber Security R&D Requirements. In 2005, DOE and DHS, in collaboration with NRCan, facilitated an industry-led effort to define the top R&D needs for improving the cyber security of the North American energy infrastructure. This effort involved industry leaders from the electricity, oil, natural gas, and communications sectors, as well as representatives from a broad cross-section of control system experts, commercial system vendors, industry associations, universities, national laboratories, and government agencies. This culminated in the January 2006 publication of the Roadmap to Secure Control Systems in the Energy Sector[42] (Control Systems Roadmap), which identifies concrete steps to secure control systems in the electricity, oil, and natural gas infrastructures over the next 10 years. This Control Systems Roadmap establishes four main cyber security goals and addresses the full spectrum of cyber security priorities in the Energy Sector, including effective practices, standards, tools, information sharing, and training. Table 7.1 highlights the resulting milestones that the sector must achieve to accomplish the 10-year vision for control systems.

[40] National Research Council, Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, 2002, www.nap.edu/catalog/10415.html?onpi_topnews090902.

[41] RAND Corporation, unpublished workshop summary.

[42] www.oe.energy.gov/DocumentsandMedia/roadmap.pdf.

Table 7.1: Strategies for Securing Control Systems in the Energy Sector

Control Systems Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.

Challenges

- Limited ability to measure and assess cyber security posture
- No consistent cyber security metrics
- Hard to quantify and demonstrate threats
- Growing risks from increasingly interconnected systems
- Poorly designed connections of control systems and business networks
- Lack of clear design requirements
- Avoidance of performance degradation via security upgrades to legacy systems
- Increasingly sophisticated hacker tools
- Insufficient information sharing
- Poor industry-government coordination
- Weak business case for cyber security investments

Control Systems Roadmap Goals

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion and Implement Response Strategies	Sustain Security Improvements

Control Systems Roadmap Milestones

Near Term (0-2 Years)

• Baseline security methodologies, vulnerability assessments, and training available	• Consistent training materials on cyber and physical security for control systems widely available within the Energy Sector	• Incident reporting guidelines published and available throughout the Energy Sector	• Major info protection and sharing issues resolved between the U.S. government and industry • Industry-driven awareness campaign launched

Mid Term (2-5 Years)

• 50% of asset owners and operators performing vulnerability assessments of their control systems using consistent criteria • Common metrics available for benchmarking security posture • 90% of Energy Sector asset owners conducting internal compliance audits	• Communication between remote access devices and control centers secure • Field-proven best practices for control system security available • Secure connectivity between business systems and control systems within corporate network	• Cyber incident response in emergency operating plans at 30% of control systems • Commercial products in production that correlate all events across the enterprise network	• Secure forum for sharing cyber threat and response information • Compelling, evidence-based business case for investment in control systems security • Undergraduate curriculums, grants, and internships in control system security • Federal and state incentives to accelerate investment in technologies and practices

Long Term (5-10 Years)

• Real-time security state monitoring for new and legacy systems commercially available	• Non-destructive intrusion, isolation, and automated response exercises at 50% of control systems • Security test harness for evaluating next generation architectures and individual components	• Control system network models for contingency and remedial action in response to intrusions and anomalies • Self configuring control system network architectures in production	• Cyber security awareness, education, and outreach programs integrated into Energy Sector operations

End State (2015)

Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation	Next-generation control system components and architectures that offer built-in, end-to-end security will replace older legacy systems	Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions	Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances

The milestones in the roadmap produced a structured, prioritized set of R&D needs that are identified in the Control Systems Roadmap. Together they provide an integrated framework to help align and coordinate industry and government R&D related to cyber security in the Energy Sector. The roadmap has received strong support from both energy SCCs and was identified by the National Infrastructure Advisory Council (NIAC) as a model for other sectors to use. Each council plans to take an active role in implementing the roadmap, which may involve the following activities:

- Mapping industry and government control systems security activities;
- Identifying gaps and overlaps;
- Refining the roadmap milestones and priorities;
- Measuring progress toward roadmap goals and milestones;
- Attracting industry and government resources to roadmap priorities; and
- Recommending and endorsing specific actions that will help industry and/or government achieve the roadmap vision and goals.

Physical Security R&D Needs. The varied nature of Energy Sector assets suggests that the types of R&D to improve physical security in the sector cover a far wider range than for cyber security. The physical assets themselves differ markedly between the electricity and the oil and natural gas subsectors. Further differences in protection opportunities are also evident among subsector components, such as substations versus transmission lines and refineries versus pipelines. While security technologies for physical assets are generally more mature than those for cyber systems, efforts to define the priority R&D needs to enhance the physical security of these diverse assets are likely to require several distinct, coordinated mapping efforts.

Using the Sector Partnership Model, DOE and the energy GCC will work closely with both energy SCCs to identify the R&D opportunities for improving physical security of the energy infrastructure. The SCCs will play pivotal roles in defining and convening the appropriate forums. Each effort will include the following steps:

- Developing a shared vision of a secure, reliable, and robust energy infrastructure and the goals to achieve it;
- Defining the boundaries for each roadmap;
- Identifying the full range of stakeholder groups that need to participate, including those from interdependent sectors;
- Engaging all stakeholders, including DHS, DOE, and other agencies; States; private industry; and academia; and broadening the partnerships to leverage the sector's limited resources;
- Developing roadmaps to meet the goals in the shared vision;
- Developing and demonstrating tools and technologies that improve the physical and cyber security of Energy Sector assets;
- Because of the urgency of the threat, emphasizing the support of tools and technologies that yield near-term responses to high-risk vulnerabilities;
- Because resources are limited, supporting activities (particularly near-term activities) that have potential for achieving a positive return on investment; and
- Because the nature of threats and vulnerabilities is continually changing, supporting intermediate and long-range R&D as identified in the roadmaps.

Integrated R&D Needs. The Energy SSP will align with the Control Systems Roadmap and the results of future efforts to define the Energy Sector's physical security R&D needs to form a unified R&D strategy.

7.3 Sector R&D Plan

Diverse public and private R&D initiatives are currently in progress to improve the Energy Sector's cyber security. DOE is working with other Federal agencies and industry groups to identify and map control system projects to R&D priorities identified in the Control Systems Roadmap. As of August 2006, DOE has identified more than 100 projects that are currently underway (appendix 8). DOE's OE is actively pursuing a broad range of projects to enhance security in the Energy Sector.

As future mapping efforts progress, new opportunities may be identified as well as common activity areas where better coordination could optimize available resources. The resulting map will be used to align and guide ongoing government and industry activities and will be updated periodically to track progress.

While formal mapping of R&D activities to address the physical security of Energy Sector assets awaits development, many important R&D activities are being conducted by industry and government. Consistent with the wide variation among assets, many of these are component-specific projects. As the energy SCCs move forward to develop R&D frameworks and mapping efforts, they will solicit active participation from a broad range of stakeholders (e.g., Interstate Natural Gas Association of America (INGAA), Electric Power Research Institute (EPRI), Gas Technology Institute (GTI), Pipeline Research Council International (PRCI), and National Electric Equipment Manufacturers Association).

7.4 R&D Management Processes

The Energy Sector will pursue a focused, coordinated management approach that: (1) aligns current activities to R&D goals and milestones, (2) initiates specific projects to address critical gaps, and (3) provides a mechanism for collaboration, project management, and oversight. The aim of this approach is to accomplish clearly defined activities, projects, and initiatives that contain time-based deliverables that are tied to priority R&D requirements.

The energy SCCs will help develop and manage an overall coordinating framework that reflects the industry's R&D priorities. Through their existing relationships throughout the sector, the SCCs can identify the appropriate R&D management structures that already exist (in organizations such as PRCI and INGAA) and incorporate them into an effective mechanism to facilitate broader coordination and leveraging of resources across the Energy Sector.

8. Managing and Coordinating SSA Responsibilities

This chapter discusses the management processes that DOE has established (or will establish) in its role as energy SSA and how it will ensure that these responsibilities are satisfied. Many of the sector's management procedures and processes are already in place. DOE will work closely with other government energy-security partners on resource issues.

8.1 Program Management Approach

DOE's Office of Electricity Delivery and Energy Reliability (OE) will manage and coordinate DOE's responsibilities as the SSA for energy. This office will designate a program manager who will oversee agency responsibilities and activities associated with NIPP and the Energy SSP. This structure will be assessed as required, along with the planned updates of the Energy SSP.

In keeping with the public-private partnership model adopted by the Energy Sector, DOE and other Federal, State, and local government energy sector partners will continue to work closely with their industry security partners to manage the SSP process and its implementation. DOE does not view this as a government program, but rather as a joint government-industry activity.

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

DOE will work closely with its security partners in both the electricity and oil and natural gas industry to update the SSP on a regular basis, at least biennially. These updates will reflect developments and lessons learned during the plan's implementation. After an initial 4-year period of regular updates, DOE and its energy security partners will update the SSP as needed to coincide with the updated NIPP Base Plan. During the review cycle, as the Base Plan is updated, DOE and its partners will make any updates or changes in coordination with DHS and other government energy security partners. Throughout this process, the DOE program manager will maintain and coordinate version control and manage comments or changes to the updated SSP. These changes will be developed and shared with all of DOE's energy security partners. DOE will continue to have the lead for maintaining and updating the plan, and all updates will be made through a collaborative process with Energy Sector security partners. In executing this process, DOE will continue to work through the CIPAC working groups for electricity and oil and natural gas, which include representatives from other concerned Federal agencies, State and local governments, and private industry partners.

8.2.2 Annual Reporting

In accordance with DHS requirements, DOE and its security partners will submit an Energy Sector CI/KR Protection Annual Report. The first of these reports was submitted in July 2006 in accordance with DHS guidance. The DOE program manager

will oversee this annual report each year. Coordination with appropriate security partners will be managed through the oil and natural gas and electric CIPAC working groups.

8.2.3 Resources and Budgets

The entire DOE OE budget for operations and analysis supports the objectives of the Sector-Specific Plan. DOE will continue to work with its sector security partners as appropriate to develop sector-specific guidance for investment priorities and requirements for CI/KR protection, restoration, and recovery.

8.2.4 Training and Education

Successful implementation of the national risk management framework relies on building and maintaining individual and organizational CI/KR protection expertise. Training and education in a variety of areas are necessary to achieve and sustain this level of expertise.

DOE will continue to develop and encourage effective training programs to help ensure widespread participation and buy-in through various industry participants. Many industry partners have sophisticated and well-developed training programs already in place, both at the company level and through industry groups. Some training, such as that for gas controllers, is mandated by regulation. NERC establishes training and certification requirements for the electricity subsector. DOE has supported training for State and local government through programs offered by NASEO, NARUC, NCSL and NGA. This has included regional training for public utility commissions by NARUC, Web-based training for EEACs offered by NASEO, and workshops and presentations conducted at meetings and conferences across the United States. In addition, regional energy emergency exercises are currently being offered.

The NIPP Base Plan lists some of the areas of expertise where training is recommended,[43] examples of available training, and other general information on CI/KR protection-related training and education. DOE will continue to work with DHS and other Energy Sector security partners to identify training needs.[44]

8.3 Information Sharing and Protection

Chapter 5 of this SSP describes various mechanisms currently in place for energy security partners to share and protect information. Considerable progress has been made in these efforts. As the SSA for energy, DOE is responsible for collaboration with private sector security partners, as well as for encouraging development of appropriate information-sharing and analysis processes and mechanisms to support these processes. DOE is undertaking these efforts with a particular focus on protection of sensitive information regarding physical and cyber threats, vulnerabilities, incidents, recommended protective measures, and security-related effective practices. The primary objective of the NIPP networked approach to information sharing is to maximize the ability of government and private sector security partners at all levels to assess risks and execute risk mitigation programs and activities.[45]

Specific information-sharing and protection plans already exist, including ESISAC, HSIN, and ISERnet.. Other mechanisms will be developed as DOE continues to work with its security partners. All efforts will be made to facilitate communication between DOE, the SCCs, governmental and private sector partners, and international partners, as appropriate.

[43] See section 6.2 of the NIPP Base Plan.
[44] For further discussions, see NIPP Base Plan, section 6.2, Enabling Education, Training, and Exercise Programs, pp. 80-83.
[45] See section 4.2, of the NIPP Base Plan.

Appendix 1: List of Acronyms and Abbreviations

AGA	American Gas Association
APGA	American Public Gas Association
API	American Petroleum Institute
APPA	American Public Power Association
BOR	Bureau of Reclamation
BPA	Bonneville Power Administration
BZPP	Buffer Zone Protection Program
CII Act	Critical Infrastructure Information Act
CI/KR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CIPC	Critical Infrastructure Protection Committee
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOS	Department of State
DOT	Department of Transportation
DPA	Defense Production Act
EEAC	Energy Emergency Assurance Coordinators
EEI	Edison Electric Institute
EIA	Energy Information Administration
EIAC	Energy Industry Assurance Coordinators
EPA	Environmental Protection Agency
EPCA	Energy Policy and Conservation Act
EPRI	Electric Power Research Institute
ERO	Energy Reliability Organization
ESCC	Electricity Sector Coordinating Council
ESF	Emergency Support Function
ESISAC	Electricity Sector Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
FPA	Federal Power Act
FUA	Power Plant and Industrial Fuel Use Act
GCC	Government Coordinating Council
GTI	Gas Technology Institute
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSAS	Homeland Security Advisory System
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IEA	International Energy Agency
IEP	International Energy Program
IFIP	Interagency Forum for Infrastructure Protection
INGAA	Interstate Natural Gas Association of America

ISAC	Information Sharing and Analysis Center
ISER	Infrastructure Security and Energy Restoration
ISO	Independent System Operator
LNG	Liquefied Natural Gas
MISO	Midwest Independent System Operator
MMS	Minerals Management Service
MOU	Memorandum of Understanding
MTSA	Maritime Transportation Security Act
NADB	National Asset Data Base
NAEWG	North American Energy Working Group
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Officials
NCS	National Communications System
NCSD	National Cyber Security Division
NCSL	National Conference of State Legislatures
NEMA	National Emergency Management Association
NEPA	National Environmental Policy Act
NERC	North American Electric Reliability Corporation
NGA	National Governors Association
NIPP	National Infrastructure Protection Plan
NPRA	National Petrochemical and Refining Association
NRC	Nuclear Regulatory Commission
NRCan	Natural Resources Canada
NRP	National Response Plan
NYMEX	New York Mercantile Exchange
O&G	Oil and Gas
OE	Office of Electricity Delivery and Energy Reliability
OIP	Office of Infrastructure Protection
PCII	Protected Critical Infrastructure Information Program
PHMSA	Pipeline and Hazardous Material Safety Administration
PMA	Power Marketing Administrations
PNWER	Pacific Northwest Economic Region
PRCI	Pipeline Research Council International
PSEPC	Public Safety and Emergency Preparedness Canada
PTI	Public Technology Institute
PURPA	Public Utilities Regulatory Policy Act
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RAM-T℠	Risk Assessment Methodology for Transmission
R&D	Research & Development
S&T	Science & Technology Directorate
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SIP	State Implementation Plan
SPP	Security and Prosperity Partnership of North America
SPR	Strategic Petroleum Reserve
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
TISP	The Infrastructure Security Partnership
TSA	Transportation Security Administration
TSI	Threats and Suspicious Incidents
TSSP	Transportation Sector-Specific Plan
TSWG	Technical Support Working Group
TVA	Tennessee Valley Authority
USACE	United States Army Corps of Engineers
USCG	United States Coast Guard
USDA	United States Department of Agriculture
WAPA	Washington Area Power Association

Appendix 2: Sources and References

American Gas Association (AGA), www.aga.org

American Petroleum Institute (API), www.api.org

American Public Gas Association (APGA), www.apga.org

American Public Power Association (APPA), www.appanet.org

Bonneville Power Administration (BPA), www.bpa.gov

California Energy Commission, www.energy.ca.gov

Canadian Electricity Association (CEA), www.canelect.ca

Critical Infrastructure Information Act of 2002 (CII Act), www.dhs.gov/xlibrary/assets/CII_Act.pdf

Critical Infrastructure Partnership Advisory Council (CIPAC), www.dhs.gov/xprevprot/committees/editorial_0843.shtm

Edison Electric Institute (EEI), www.eei.org

Electric Power Research Institute (EPRI), www.epri.com

Electricity Sector Information Sharing and Analysis Center (ESISAC), www.esisac.com

Energy Policy Act of 2005 (EPAct 2005),
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6enr.txt.pdf

Energy Reliability Organization (ERO), www.nerc.com/about/ero.html

Federal Emergency Management Agency (FEMA), www.fema.gov

Federal Energy Regulatory Commission (FERC), www.ferc.gov

Final Report on the August 14th Blackout in the United States and Canada (Blackout Report), https://reports.energy.gov

Gas Technology Institute (GTI), www.gastechnology.org

Homeland Security Advisory System (HSAS), www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

Homeland Security Information Network (HSIN), www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm

Homeland Security Presidential Directive 7 (HSPD-7), www.whitehouse.gov/news/releases/2003/12/20031217-5.html

Infrastructure Security and Energy Restoration (ISER), www.oe.netl.doe.gov/about.asp

Interstate Natural Gas Association of America (INGAA), www.ingaa.org

Minerals Management Service (MMS), www.mms.gov

National Association of Regulatory Utility Commissioners (NARUC), www.naruc.org

National Association of State Energy Officials (NASEO), www.naseo.org

National Conference of State Legislatures (NCSL), www.ncsl.org

National Governors Association (NGA), www.nga.org

National Infrastructure Protection Plan (NIPP), www.dhs.gov/xprevprot/programs/editorial_0827.shtm

National Petrochemical and Refiners Association (NPRA), www.npradc.org

National Propane Gas Association, www.npga.org

National Rural Electric Cooperative Association, www.nreca.org

National Science Foundation, www.nsf.gov

Natural Resources Canada (NRCan), www.nrcan.gc.ca

NERC Critical Infrastructure Protection Committee (CIPC), www.nerc.com/~filez/cip.html

NERC Reliability Standards, https://standards.nerc.net

North American Electric Reliability Corporation (NERC), www.nerc.com

North American Energy Standards Board, www.gisb.org

North American Energy Working Group (NAEWG), www.eia.doe.gov/emeu/northamerica/engnaewg.htm#_VPID_1

Nuclear Regulatory Commission (NRC), www.nrc.gov

Office of Electricity Delivery and Energy Reliability (OE), www.oe.energy.gov

Office of Science and Technology Policy (OSTP), www.ostp.gov

Pacific Northwest Economic Region (PNWER), www.pnwer.org

Pipeline and Hazardous Materials Safety Administration (PHMSA), www.phmsa.dot.gov

Power Marketing Administration (PMA), ww.energy.gov/organization/powermarketingadmin.htm

Protected Critical Infrastructure Information (PCII) Program, www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

Public Safety and Emergency Preparedness Canada (PSEPC), www.psepc-sppcc.gc.ca

Public Technology Institute (PTI), www.pti.org

Regional Transmission Organization, www.ferc.gov/industries/electric/indus-act/rto.asp

Strategic Petroleum Reserve (SPR), www.spr.doe.gov

Technical Support Working Group (TSWG), www.tswg.gov/tswg/home/home.htm

Tennessee Valley Authority (TVA), www.tva.gov

The Electric Distribution Program (GridWise Program), www.electricdistribution.ctc.com/index.htm

The Infrastructure Security Partnership (TISP), www.tisp.org/tisp.cfm

Transportation Security Administration (TSA), www.tsa.gov

United States Army Corps of Engineers (USACE), www.usace.army.mil

United States Coast Guard (USCG), www.uscg.mil

United States Department of Agriculture (USDA), www.usda.gov

United States Department of Commerce (DOC), www.commerce.gov

United States Department of Defense (DOD), www.defenselink.mil

United States Department of Energy (DOE), www.doe.gov

United States Department of Energy, Energy Information Administration (EIA), www.eia.doe.gov

United States Department of Homeland Security (DHS), www.dhs.gov/dhspublic

United States Department of the Interior (DOI), www.doi.gov

United States Department of the Interior, Bureau of Reclamation (BOR), www.usbr.gov

United States Department of State (DOS), www.state.gov

United States Department of Transportation (DOT), www.dot.gov

United States Environmental Protection Agency (EPA), www.epa.gov

Western Area Power Administration (WAPA), www.wapa.gov

Appendix 3: Authorities

A.1 Authorities Affecting Multiple Segments of the Energy Sector

Homeland Security Presidential Directive 5

This directive enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system. It requires all Federal departments and agencies to cooperate with the Secretary of Homeland Security by providing their full and prompt cooperation, resources, and support, as appropriate and consistent with their own responsibilities for protecting the Nation's security. The directive provides for Federal assistance to State and local authorities when their resources are overwhelmed, or when Federal interests are involved.

Homeland Security Presidential Directive 7

This directive establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks. Federal departments and agencies are required to: (1) identify, prioritize, and coordinate CI/KR protection in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them; and (2) work with State and local governments and the private sector to accomplish this objective. Federal departments and agencies are directed to protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of CI/KR consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Federal Information Security Management Act of 2002 (FISMA); E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) (December 16, 2003); FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (February 10, 2004); National Information Assurance Acquisition Policy for National Security Systems (NSTISSP 11); Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations (June 2004)

DOE, like other Federal agencies, is responsible for complying with FISMA as well as guidelines and practices developed by OMB that implement the law. While FISMA applies strictly to Federal Government agencies, DOE has carefully implemented requirements that support protection of the energy infrastructure. These include, for example, OMB's e-authentication guidance for remote authentication, National Institute of Standards and Technology guidelines for securing and procuring national security systems, and other related guidance.

Protected Critical Infrastructure Information Program of the Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-134

The PCII Program, established pursuant to the CII Act, creates a framework that enables members of the private sector to voluntarily submit sensitive information regarding the Nation's critical infrastructure to DHS with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure. To implement and manage the program, DHS has created the PCII Program Office within DHS's National Protection and Programs Directorate. The PCII Program Office or other Federal agencies designated by the PCII program manager can receive critical infrastructure information to be validated as PCII if such information qualifies for protection under the CII Act. On September 1, 2006, DHS issued a Final Rule on Procedures for Handling Critical Infrastructure Information.

Bonneville Project Act of 1937, 16 U.S.C. 832 et seq.; Reclamation Act of 1939, as amended, 43 U.S.C. 584 et seq.; Flood Control Act of 1944, 16 U.S.C. 825(s); Colorado River Storage Act of 1956, 43 U.S.C. 620 et seq.; Pacific Northwest Preferences Act of 1964, 16 U.S.C. 837; Federal Columbia River Transmission System Act of 1974, 16 U.S.C. 838; Department of Energy Organization Act, Section 302, 42 U.S.C. 7152; Pacific Northwest Electric Planning and Conservation Act of 1980, 16 U.S.C. 839; and Energy and Water Development Appropriation Act of 1985, 16 U.S.C. 837g-1

DOE's PMAs have general powers under enabling legislation to manage multiple areas of CIP. These range from protection to response and restoration covering generation, transmission, and related facilities. Congress provides similar authority to the Tennessee Valley Authority (TVA) to protect and reconstitute TVA generation, transmission, and related facilities.

Federal Power Act (FPA), 16 U.S.C. 791a-825r; Public Utility Regulatory Policies Act (PURPA) of 1978, codified in 16 U.S.C. 2601 et seq.; Energy Policy Act of 1992, 42 U.S.C. 13201 note

Congress provides a statutory foundation for FERC's oversight of power markets. While generation siting, intrastate transportation, and retail sales are generally regulated by State or local entities, wholesale sales and interstate transportation generally fall under Federal regulation, primarily by FERC.

One of FERC's strategic goals is to protect customers and market participants through vigilant and fair oversight of energy markets in transition. To pursue this goal, the Commission promotes understanding of energy market operations and assesses market conditions using objective benchmarks to create pro-competitive market structure. FERC's Office of Market Oversight and Investigations is charged with assessing the competitive performance and efficiency of U.S. wholesale natural gas and electricity markets.

Federal Power Act, as amended, 202(a) (16 U.S.C. 791a), and the Public Utility Regulatory Policies Act, Section 209(b) (16 U.S.C. 824a-2)

The Secretary of Energy has authority with regard to reliability of the interstate electric power transmission system. DOE has the authority to define reliability regions and encourage interconnection and coordination within and between regions. DOE also has the authority to gather information regarding reliability issues and to make recommendations regarding industry security and reliability standards.

Defense Production Act (DPA) of 1950, as amended, 101(a), 101(c), and 708 (50 U.S.C. 2071 (a), (c), and 2158)

The Secretaries of Energy and Commerce have been delegated the President's authorities under sections 101(a) and 101(c) of DPA to require the priority performance of contracts or orders relating to materials (including energy sources), equipment, or services, including transportation, or to issue allocation orders, as necessary or appropriate for the national defense or to maximize domestic energy supplies. DPA section 101(a) permits the priority performance of contracts or orders necessary

or appropriate to promote the national defense. "National defense" is defined in DPA section 702(13) to include "emergency preparedness activities conducted pursuant to title VI of the Robert T. Stafford Disaster Relief and Emergency Act and critical infrastructure protection and assurance." The Secretary of Energy has been delegated (Executive Orders 12919 and 11790) the DPA section 101(a) authority with respect to all forms of energy. The Secretary of Commerce has been delegated (Executive Order 12919) the section 101(a) authority with respect to most materials, equipment, and services relevant to repair of damaged energy facilities. Section 101(c) of the DPA authorizes contract priority ratings relating to contracts for materials (including energy sources), equipment, or services in order to maximize domestic energy supplies, if the Secretaries of Commerce and Energy, exercising their authorities delegated by Executive Order 12919, make certain findings with respect to the need for the material, equipment, or services for the exploration, production, refining, transportation, or conservation of energy supplies.

The DPA priority contracting and allocation authorities could be used to expedite repairs to damaged energy facilities, and for other purposes, including directing the supply or transportation of petroleum products, to maximize domestic energy supplies, meet defense energy needs, or support emergency preparedness activities. In the case of both the section 101(a) and 101(c) authorities, if there are contracts in place between the entity requiring priority contracting assistance and one or more suppliers of the needed good or service, DOE (with respect to the section 101(c) authority) or DOC (with respect to the section 101(a) authority) would issue an order requiring suppliers to perform under the contract on a priority basis before performing other non-rated commercial contracts. If no contracts are in place, DOE or DOC would issue a directive authorizing an entity requiring the priority contracting assistance to place a rated order with a supplier able to provide the needed materials, equipment, or services. That contractor would be required to accept the order and place it ahead of other nonrated commercial orders.

DPA section 708 provides a limited antitrust defense for industry participating in voluntary agreements "to help provide for the defense of the United States through the development of preparedness programs and the expansion of productive capacity and supply beyond levels needed to meet essential civilian demand in the United States." In the event of widespread damage to energy production or delivery systems, this authority, for example, could be used to establish a voluntary agreement of service companies to coordinate the planning of the restoration of the facilities.

Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. 5121 et seq.

FEMA, following a presidential declaration of emergency or major disaster, provides assistance and may require other Federal agencies to provide resources and personnel to support State and local emergency and disaster assistance efforts. Requests for a presidential declaration of an emergency or major disaster must be made by the Governor of the affected State based on a finding by the Governor that the situation is of such severity and magnitude that effective response is beyond the capabilities of the State. DOE supports DHS/ FEMA relief efforts by assisting Federal, State, and local government and industry with their efforts to restore energy systems in disaster areas. When necessary, DOE also may deploy response staff to disaster sites. DOE is the lead agency directing Emergency Support Function-12 (Energy), which assists the restoration of energy systems and provides an initial point-of-contact for the activation and deployment of DOE resources. These activities are performed pursuant to the Stafford Act and HSPD-5 (Management of Domestic Incidents) and NRP.

Executive Order 11912, Department of Energy Organization Act, Sections 102 and 203 (42 U.S.C. 7112, 7133); Energy Policy and Conservation Act (EPCA), Sections 251-254 (42 U.S.C. 6271-6274); Agreement on an International Energy Program (IEP)

DOE and DOS share responsibility for U.S. participation in the energy emergency preparedness activities of the International Energy Agency (IEA). IEA, consisting of 26 member countries, was established by IEP following the 1973 oil crisis with the goal of developing and maintaining cooperative oil emergency response policies and programs. DOE leads U.S. participation in IEA's oil emergency response programs. The Department develops plans for U.S. emergency response actions, develops the U.S. position on an appropriate international response, and makes recommendations for action to the President.

Section 27 of the Merchant Marine Act of 1920, as amended (Jones Act), 46 U.S.C. 883

Public Law 81-891(64 Stat. 1120) directs the Secretary of Homeland Security to waive the provisions of section 27 of the Merchant Marine Act of 1920 ("Jones Act") which requires the use of U.S.-flag, U.S.-built, and U.S.-crewed vessels in coastwise trade, upon the request of the Secretary of Defense to the extent the Secretary of Defense deems necessary in the interest of the national defense. Public Law 81-891 authorizes the Secretary of Homeland Security to waive compliance with the Jones Act either upon his own initiative or upon the written recommendation of the head of another agency whenever the Secretary determines that waiver is necessary in the interest of the national defense. In the event of a drawdown of SPR, the President may direct the Secretary of Homeland Security to waive the Jones Act, if the volume of crude oil to be moved is significantly greater than the capacity of the existing, available U.S.-flag "Jones Act" crude oil tanker fleet. Interagency procedures have been established to expedite actions on Jones Act waiver requests during a petroleum supply disruption.

Ports and Waterways Safety Act, Natural Gas Pipeline Safety Act, and the Hazardous Liquids Pipeline Safety Act, 33 U.S.C. 1221 et seq.

The Ports and Waterways Safety Act authorizes the Secretary of Transportation to establish vessel traffic systems for ports, harbors, and other navigable waters and control vessel traffic in areas determined to be hazardous (e.g., because of conditions of reduced visibility, adverse weather, vessel congestion, etc.) (33 U.S.C. 1223).

Two statutes provide the framework for the Federal pipeline safety program. The Natural Gas Pipeline Safety Act of 1968 as amended authorizes DOT to regulate pipeline transportation of natural (flammable, toxic, or corrosive) gas and other gases as well as the transportation and storage of LNG. Similarly, the Hazardous Liquid Pipeline Safety Act of 1979 as amended authorizes DOT to regulate pipeline transportation of hazardous liquids (crude oil, petroleum products, anhydrous ammonia, and carbon dioxide). Both of these Acts have been recodified as 49 U.S.C. Chapter 601. The Federal pipeline safety regulations (1) assure safety in design, construction, inspection, testing, operation, and maintenance of pipeline facilities in the siting, construction, operation and maintenance of LNG facilities; (2) set out parameters for administering the pipeline safety program; and (3) delineate requirements for onshore oil pipeline response plans. The regulations are written as minimum performance standards.

The Magnuson Act (50 U.S.C. 191 et seq.) directs the Secretary of Transportation to issue regulations governing the movement of any vessel within U.S. Territorial waters, upon a presidential declaration of a national emergency by reasons of actual or threatened war, insurrection or invasion, or disturbance or threatened disturbance of the international relations of the United States (50 U.S.C. 191).

Maritime Transportation Security Act (MTSA), Public Law 107-295, 46 U.S.C. 2101 note

MTSA, which amended the Merchant Marine Act of 1936, requires implementation of regulations for improving the security of ports, waterfront facilities, and vessels, including those involved with the oil and gas sectors. Most energy sites with waterfront facilities are impacted by MTSA and must conduct vulnerability assessments and develop security plans to be approved by the USCG.

Communications Act of 1934, 47 U.S.C. 151 et seq., as amended, and Executive Order 12472, as amended

The National Security Emergency Preparedness Telecommunications Service Priority System, created by the National Communications System (NCS), an interagency body established by Executive Order 12472, authorizes priority treatment for restoration and provisioning (installation of new service) of certain domestic telecommunication services during several categories of emergency. Under this program, DOE is authorized to sponsor energy industry requests for priority restoration of existing telecommunications or requests for priority installation of new telecommunications as well as priority access to the Public Switch Network. Authority to order priority restoration of electric service resides in the States rather than the Federal

Government. DOE, in its role supporting FEMA and DHS under NRP as ESF-12, has been successful in requesting and obtaining priority restoration of electric service for specific important electric loads and areas.

Aviation and Transportation Security Act (ATSA), Public Law 107-71, 115 Stat. 597, November 19, 2001

As established by ATSA, TSA is responsible for security in all modes of transportation. The six modes of transportation include mass transit, aviation, maritime, highway, rail, and pipeline systems. As further noted in NIPP, TSA is the SSA for all modes of transportation except maritime, for which the USCG is the SSA.

Critical Energy Infrastructure Information, FERC Orders 630 and 630A

FERC issued a final rule restricting access to Critical Energy Infrastructure Information and establishing new procedures for requesting access to Critical Energy Infrastructure Information.

A.2 Authorities Affecting Electric Power

Energy Policy Act of 2005, Public Law 109-58, Title XII: Electricity, Subtitle A: Reliability Standards, Section 1211: Electric Reliability Standards; Electricity Modernization Act of 2005, August 5, 2005, 42 U.S.C. 15801 note; 16 U.S.C. 824o

This subtitle provides for Federal jurisdiction over certain activities that are required to support reliability of the U.S. bulk power system. Title XII authorizes FERC to certify a national electric reliability organization to enforce mandatory reliability standards for the bulk power system. FERC will oversee the electric reliability organization in the U.S. and all electric reliability organization standards must be approved by FERC. The electric reliability organization can impose penalties on a user, owner, or operator of the bulk power system for violations of any FERC-approved reliability standard, but such penalties are subject to FERC review and potential change.

FERC Order Issued in Docket No. RR06-1-000, Certifying NERC as the Electric Reliability Organization, July 20, 2006

Pursuant to the EPAct of 2005, FERC conditionally certified NERC as the Nation's ERO. NERC must make specified changes to the electric reliability organization and file those changes with FERC in order to continue as the electric reliability organization. As the electric reliability organization, NERC will be responsible for developing and enforcing mandatory electric reliability standards under the FERC's oversight. The standards will apply to all users, owners, and operators of the bulk power system.

Federal Power Act, 16 U.S.C. 791a-825r; Public Utility Regulatory Policies Act, 16 U.S.C. 2705; DOE Organization Act, 42 U.S.C. 7101-7352; 18 CFR Parts 4, 12, and 16; MOU between FERC and Army Corps of Engineers and Bureau of Reclamation

Congress authorizes FERC to oversee the Nation's nonfederal hydropower infrastructure. Congressional and other legal delegations also define hydropower responsibilities among FERC and other agencies, such as USACE and BOR.

With regard to FERC authorities, delegations in FPA include a range of activities, such as issuing licenses for nonfederal hydropower projects; requiring safety and operating conditions; investigating and taking over facilities (or levying fines) for administrative violations, such as safety and security; defining construction, maintenance, and operation requirements by licensees; and other acts to carry out the purposes of the Federal Power Act. In addition, section 405(d) of PURPA, 16 U.S.C. 2705, authorizes a hydropower project's exemption from licensing under certain conditions. Finally, DOE Organization Act, 42 U.S.C. 7101-7352: Title IV establishes FERC (as the successor agency to the Federal Power Commission) and enumerates FERC's authority regarding hydropower facilities.

In addition to congressional delegations, regulations further define FERC authorities over hydropower facilities. These rules address such issues as project safety and security, procedures for relicensing or Federal takeover of licensed hydropower projects, and investigations.

FERC has several MOUs with regard to hydropower facilities:

- **USACE**, which has responsibility for ownership and operation of Federal dams for electric power production and other purposes. This MOU describes procedures for agency cooperation during the processing of hydropower applications to facilitate the investigation, construction, operation, and maintenance of FERC-licensed hydro projects at USACE dams.
- **BOR**, which has responsibility for ownership and operation of dams for electric power production and other purposes. This MOU describes procedures for agency cooperation during the processing of hydropower applications to facilitate the investigation, construction, operation, and maintenance of FERC-licensed hydro projects at BOR dams.

Executive Order 10485, Providing for the Performance of Certain Functions Heretofore Performed by the President with Respect to Electric Power and Natural Gas Facilities Located on the Borders of the United States, September 3, 1953, as amended by Executive Order 12038, Relating to Certain Functions Transferred to the Secretary of Energy by the Department of Energy Organization Act, February 3, 1978

DOE is authorized to issue presidential permits for the construction, operation, maintenance, and connection of electric transmission facilities at U.S. international borders if it determines that the issuance of such a permit is in the public interest. In determining whether issuance of the permit is consistent with the public interest, DOE considers the impact the proposed project would have on the operating reliability of the U.S. electric power supply and the environmental impacts of the proposed project pursuant to the National Environmental Policy Act (NEPA) of 1969, and any other factors that DOE may also consider relevant to the public interest. DOE must also obtain favorable recommendations from the Secretary of State and Secretary of Defense before issuing a permit.

Federal Power Act, as amended, 202(c), 16 U.S.C. 824a(c)

The Secretary of Energy has authority in time of war or other emergency to order temporary interconnections of facilities and generation, delivery, interchange, or transmission of electric energy that the Secretary deems necessary to meet an emergency. This authority may be utilized upon receipt of a petition from a party requesting the emergency action or it may be initiated by DOE on its own initiative.

Federal Power Act, as amended, 202(e), 16 U.S.C. 824a(e)

Exports of electricity from the United States to a foreign country are regulated by DOE pursuant to sections 301(b) and 402(f) of the Department of Energy Organization Act (42 U.S.C. 7151(b), 7172(f)) and require authorization under section 202(e) of FPA (16 U.S.C. 824a(e)).

Department of Energy Organization Act and FPA, 10 CFR 205.350-205.353

DOE has authority to obtain current information regarding emergency situations on the electric supply systems in the United States. DOE has established mandatory reporting requirements for electric power system incidents or possible incidents. This reporting is required to meet DOE's national security requirements and other responsibilities contained in NRP.

Power Plant and Industrial Fuel Use Act (FUA), 404(a), 42 U.S.C. 8374(a)

Under section 404(a), the President has authority by order to allocate coal (and require the transportation of coal) for use by any power plant or major fuel-burning installation during a declared severe energy supply interruption as defined by section

3(8) of the Energy Policy and Conservation Act, 42 U.S.C. 6202(8). The President may also exercise such allocation authority upon a published finding that a national or regional fuel supply shortage exists or may exist that the President determines is, or is likely to be, of significant scope and duration, and of an emergency nature; causes, or may cause, major adverse impact on public health, safety, welfare or on the economy; and results, or is likely to result, from an interruption in the supply of coal or from sabotage, or from an act of God. Section 404(e) stipulates that the President may not delegate his authority to issue orders under this authority. It does not, however, prevent the President from directing any Federal agency to issue rules or regulations, or take other action consistent with section 404, in the implementation of such order.

The FUA section 404(a) authority could be used to help provide coal as an alternative fuel source to electric power plants and other major fuel-burning installations that have received orders prohibiting the burning of natural gas or petroleum as a primary energy source, assuming these facilities actually have the capability to burn coal. Many likely do not, so the authority may be of limited utility. This authority also could be used during a coal supply shortage to ensure that coal-burning electric power plants or major fuel-burning installations have adequate supplies of coal.

As an alternative to the use of FUA section 404(a), the President, or the President's delegate(s), could allocate coal supplies under the authority of section 101(a) of the Defense Production Act, 50 U.S.C. App. 2071(a) and Executive Order 12919 (1994).

Clean Air Act, 42 U.S.C. 7401 et seq.

Section 110(f) of the Clean Air Act permits a State Governor to issue an emergency temporary suspension of any part of a State Implementation Plan (SIP) (as well as a temporary waiver of penalties for excess SOx or NOx emissions) in accordance with the following: (1) the owner/operator of a fuel-burning source petitions the State for relief; (2) the Governor gives notice and opportunity for public hearing on the petition; (3) the Governor finds that an emergency exists in the vicinity of the source involving high levels of unemployment or loss of necessary energy supplies for residential dwellings, and that the unemployment or loss can be totally or partially alleviated by an emergency suspension of SIP requirements applicable to the petitioning source; (4) the President, in response to the Governor's request, declares a national or regional emergency exists of such severity that a temporary SIP suspension may be necessary and other means of responding to the energy emergency may be inadequate; and (5) the Governor issues an emergency suspension to the source. DOE may be asked to advise the President of fuel supply situations regarding requests for presidential emergency declarations for SIP relief.

A.3 Authorities Affecting Natural Gas

Natural Gas Act, Sections 3 and 7, 15 U.S.C. 717 et seq.

DOE has authority under section 3 to issue orders, upon application, to authorize imports and exports of natural gas. Section 3 requires DOE to approve, without modification or delay, applications to import LNG and applications to import and export natural gas from and to countries with which there is a free-trade agreement in effect requiring national treatment for trade in natural gas. Section 7 provides FERC the authority to approve the siting of and abandonment of interstate natural gas facilities, including pipelines, storage, and LNG facilities. FERC authority under the Natural Gas Act is to review and evaluate certificate applications for facilities to transport, exchange, or store natural gas; acquire, construct, and operate facilities for such service; and to extend or abandon such facilities. In this context, FERC approvals include the siting of said facilities and evaluation of alternative locations. FERC jurisdiction does not include production, gathering, or distribution facilities, or those strictly for intrastate service. In reference to regulating imports and exports of natural gas under section 3 of the Natural Gas Act, Executive Order 10485, as amended by Executive Order 12038, and sections 301(b), 402(e), and (f) of the Department of Energy Organization Act (42 U.S.C. 7101 et seq.), the Secretary has delegated to FERC authority over the construction, operation, and siting of particular facilities, and with respect to natural gas, that involves the construction of new domestic facilities, the place of entry for imports or exit for exports. FERC also has authority to approve or deny an application for the siting, construction, expansion, and operation of an LNG terminal under section 3 of the Natural Gas Act.

Natural Gas Policy Act, Title III, Sections 301-303, 15 U.S.C. 717 et seq.

DOE may order any interstate pipeline or local distribution company served by an interstate pipeline to allocate natural gas in order to assist in meeting the needs of high-priority consumers during a natural gas emergency. DOE has delegated authority (Executive Order 12235) under sections 302 and 303, respectively, of the Natural Gas Policy Act, to authorize purchases of natural gas and to allocate supplies of natural gas in interstate commerce to assist in meeting natural gas requirements for high-priority uses, upon a finding by the President under section 301 of an existing or imminent natural gas supply emergency (15 U.S.C. 3361-3363). The declaration of a natural gas supply emergency is the legal precondition for the emergency purchase and allocation authority in sections 302 and 303, respectively, of the Natural Gas Policy Act.

Although Executive Order 12235 delegates to the Secretary of Energy the emergency purchase and allocation authorities in sections 302 and 303, respectively, the President has not delegated his authority to declare a natural gas supply emergency. Nothing in the Natural Gas Policy Act would preclude such a presidential delegation.

Under section 301 of the Natural Gas Policy Act, the President may declare a natural gas supply emergency if he makes certain findings. The President must find that a severe natural gas shortage, endangering the supply of natural gas for high-priority uses, exists or is imminent in the United States or in any region of the country. Further, the President must find that the exercise of the emergency natural gas purchase authority under section 302 of the Natural Gas Policy Act, of the emergency allocation authority under section 303 of the Natural Gas Policy Act, or of the emergency conversion authority of section 607 of PURPA is reasonably necessary, having exhausted other alternatives to the maximum extent practicable, to assist in meeting natural gas requirements for high-priority uses. The emergency terminates on the date the President finds that a shortage either no longer exists or is not imminent, or 120 days after the date of the emergency declaration, whichever is earlier.

Public Utility Regulatory Policies Act of 1978, Section 607, 15 U.S.C. 717z, and Section 404(b) of the Power Plant and Industrial Fuel Use Act, 42 U.S.C. 8374(b)

There are two authorities that can be used in emergency situations to require utilities to switch from natural gas and petroleum for electric power generation. DOE has delegated authority (Executive Order 12235) under section 607(a) of PURPA, following the President's finding of a natural gas supply emergency, to prohibit the burning of natural gas by any electric power plant or major fuel-burning installation. The required emergency finding is identical to that in the Natural Gas Policy Act (15 U.S.C. 717z). As explained in the previous section discussing the Natural Gas Policy Act, under section 301 of the Natural Gas Policy Act and 607(a) of PURPA, the President may declare a natural gas supply emergency if he makes certain findings. The President must find that a severe natural gas shortage, endangering the supply of natural gas for high-priority uses, exists or is imminent in the United States. The PURPA fuel-switching authority is similar to the presidential authority contained in section 404(b) of the Power Plant and Industrial Fuel Use Act (FUA), 42 U.S.C 8374(b), to prohibit the burning of natural gas or petroleum by electric power plants or major fuel-burning installations.

Section 404(b) of FUA provides that the President may by order prohibit the use by any power plant or major fuel-burning installation of petroleum or natural gas, or both, as a primary energy source. A legal precondition to such a presidential order is the President's finding of a severe energy supply interruption, as defined by section 3(8) of EPCA, 42 U.S.C. 6202(8). Section 404(e) stipulates that the President may not delegate his authority to issue orders under this authority. It does not, however, prevent the President from directing any Federal agency to issue rules or regulations, or take other action consistent with section 404, in the implementation of such order.

Emergency Reconstruction, FERC Order 633

Amended FERC regulations enable interstate natural gas pipeline companies to replace mainline facilities using, if necessary, a route other than the existing right-of-way and waiving the 45-day prior notice requirement and cost constraints, when immediate action is required to restore service in an emergency because of a sudden unanticipated loss of natural gas or capacity in order to prevent loss of life, impairment of health, or damage to property. In such emergencies, the amended regulations allow pipeline companies to proceed with construction before the end of the separate 30-day prior notice period to landowners if all necessary easements have been obtained. This initiative was implemented in the wake of the events of September 11, 2001, to help ensure the security of the natural gas pipeline infrastructure without compromising the FERC's responsibilities under the NEPA.

A.4 Authorities Affecting Petroleum

Energy Policy and Conservation Act, Sections 151-180, 42 U.S.C. 6231-6251

Sections 151-191 of EPCA authorize DOE to establish and operate the SPR. Section 161(d)(1) authorizes the President to order drawdown and sale of products from the SPR upon a finding that drawdown is required either by a "severe energy supply interruption" or obligations of the United States under the Agreement on an International Energy Program (42 U.S.C. 6241(d)(1)).

Section 161(h) empowers the President to drawdown the SPR in circumstances other than a "severe energy supply interruption" or a need to meet U.S. obligations under IEP, if the President finds that a circumstance "exists that constitutes, or is likely to become, a domestic or international energy supply shortage of significant scope and duration" and the President determines that drawdown "would assist directly or significantly in preventing or reducing the adverse impact of such a shortage" and the Secretary of Defense has found that the action taken will not impair national security. However, there are several limitations on the use of this authority: The reserve may not be drawn down for more than 30 million barrels or for longer than 60 days with respect to a single event, or if the reserve would be reduced below the level of 500 million barrels (42. U.S.C. 6241(h)). EPCA gives the President authority to authorize the export of crude oil withdrawn from the SPR during a drawdown for refining or exchange outside the United States in connection with an arrangement for the delivery of refined petroleum products to the United States (42. U.S.C. 6241(i)). In recognition of this authority, DOC has provided for automatic approval for export of SPR oil for these purposes in its Export Administration Regulations at 15 CFR Part 754.

The sale of oil withdrawn from the SPR would be in accordance with the SPR competitive sales procedures in 10 CFR Part 625.

Energy Policy and Conservation Act, Sections 181-184, 42 U.S.C. 6250-6250c

Pursuant to section 181 of EPCA, 42 U.S.C. 6250, the Secretary established and maintains a 2 million barrel home heating oil reserve in the Northeast. This reserve is not part of the SPR. The Secretary may sell products from the Northeast Home Oil Reserve dependent on a presidential finding that there is a "severe energy supply interruption" in accordance with section 183(a) of the EPCA, based upon a finding that a dislocation in the heating oil market has resulted from such interruption or the existence of a regional supply shortage of significant size and duration, and that action under this section would assist directly and significantly in reducing the adverse impact of such shortage.

Section 363 of the Energy Policy and Conservation Act, 42 U.S.C. 6322(e)

To be eligible for financial assistance to assist in the development and implementation of energy conservation plans, a State must submit to the Secretary of Energy, as a supplement to its energy conservation plan, an energy emergency planning program for an energy supply disruption as designated by the State consistent with applicable Federal and State law. The contingency plan, "... shall include an implementation strategy or strategies (including regional coordination) for dealing with energy emergencies."

Appendix 4: Asset Ownership

Major energy asset ownership includes the following entities:

- **Federal Government.** The Federal Government is a major owner of energy assets and critical infrastructure throughout the United States and its Territories. Examples include the Tennessee Valley Authority, a major owner of hydroelectric dams, nuclear and fossil power generation stations, and high-voltage transmission; the Bureau of Reclamation, a major dam owner; DOE, which oversees the SPR and the Northeast Home Heating Oil Reserve; and power administrations such as Western Area Power Administration and Bonneville Power Administration.
- **State and local government.** State and especially local governments own substantial energy assets. These include all municipal utilities, many of which own generation and electric and/or natural gas distribution systems and are primarily self-regulated.
- **Regulated utilities.** Regulated utilities own most of the electric and natural gas infrastructure in the United States, and although they are private sector entities, most are rate-regulated at the Federal, State, and/or local levels. Included in this category are major interstate pipeline companies, hydroelectric facilities, storage facility operators, and LNG terminal owners, all of which are regulated by FERC.
- **Unregulated energy companies.**[46] Unregulated energy companies are those whose rates are not directly regulated by FERC or a State public utility commission and therefore charge market-based rates for the power they produce. Many of these companies own energy infrastructure assets, such as merchant generation companies owning power plants that participate in wholesale power markets. Unregulated marketing and trading companies are also active in acquiring, storing, and trading natural gas, crude oil, electricity, and petroleum products.
- **Unregulated nonenergy companies**. Unregulated, nonenergy, private sector companies, like those in the chemical, aluminum, forest products, and telecommunications industries, own energy assets including generation plants, refineries, and oil and gas production facilities.
- **Cooperatives.** Significant energy infrastructure is owned by cooperatives, especially in the electric distribution sector. These assets, which can include generation, transmission, and distribution, are generally "nonjurisdictional," meaning their rates are not regulated by FERC or the States.
- **Foreign entities.** Some U.S. energy infrastructure is owned by foreign energy concerns, including several utilities, power stations, and other asset classes. Many U.S. energy companies also own energy infrastructure in foreign countries. These U.S.-owned foreign assets may or may not be directly related to meeting energy supply needs in the United States.

[46] EPAct of 2005 mandated that FERC establish an ERO with powers to enforce rules affecting the reliability of the Nation's electric grid. NERC has been designated by FERC as the ERO. All users of the Nation's high-voltage electric grid will be subject to these mandatory reliability rules, even if they are not otherwise regulated by FERC for rates or tariffs.

Appendix 5: Energy SCC and GCC Membership and Participation

Table A5-1: Organizational Membership on Energy SCC and GCC Membership and Participation[47]

Members of the Electricity Sector Coordinating Council
American Public Power Association
Edison Electric Institute
National Rural Electric Cooperative Association
North American Electric Reliability Corporation
Members of the Oil and Natural Gas Sector Coordinating Council
American Gas Association
Association of Oil Pipe Lines
American Public Gas Association
American Petroleum Institute
Canadian Association of Petroleum Producers
Center for Liquefied Natural Gas
Domestic Petroleum Council
Gas Processors Association
International Association of Drilling Contractors
Independent Liquid Terminals Association

[47] For company participation, see www.dhs.gov/xprevprot/committees/editorial_0848.shtm.

Independent Petroleum Association of America
Interstate Natural Gas Association of America
National Association of Convenience Stores
National Ocean Industries Association
National Petrochemical & Refiners Association
National Propane Gas Association
Offshore Marine Service Association
Petroleum Marketers Association of America
Society of Independent Gasoline Marketers of America
U.S. Oil & Gas Association
Western States Petroleum Association
Participants in the Energy Government Coordinating Council
United States Army Corps of Engineers
United States Department of Agriculture, Rural Utilities Service
United States Department of Defense
United States Department of Energy, Office of Electricity Delivery and Energy Reliability
United States Department of Energy, Office of Fossil Energy
United States Department of Homeland Security, Office of Infrastructure Protection
United States Department of Homeland Security, Transportation Security Administration
United States Department of Homeland Security, United States Coast Guard
United States Department of the Interior, Minerals Management Service
United States Department of State, International Boundary and Water Commission
United States Department of Transportation, Committee on the Marine Transportation System
United States Department of Transportation. Maritime Administration
United States Department of Transportation, Pipeline and Hazardous Materials Safety Administration

United States Department of the Treasury
United States Environmental Protection Agency
Federal Energy Regulatory Commission
National Association of Regulatory Utility Commissioners
National Association of State Energy Officials

Appendix 6: Transportation SSP: Pipeline Modal Implementation Plan Executive Summary

Each day, thousands of businesses and millions of people rely on the safe, secure, and efficient movement of commodities through the transportation system. Manmade or natural disruptions to this critical system could result in significant harm to the social and economic well-being of the country. The Nation's pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements.

As required by Executive Order 13416, the Pipeline Modal Annex implements the Transportation Systems Sector-Specific Plan (SSP), and was developed to ensure the security and resiliency of the pipeline mode. The vision of this plan is to ensure that the pipeline sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, mitigate the adverse consequences of an incident, and quickly restore pipeline service.

The Transportation Systems SSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Systems Sector and Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. In accordance with the National Infrastructure Protection Plan (NIPP), a Critical Infrastructure Partnership Advisory Council (CIPAC) Oil and Natural Gas (ONG) Joint Sector Committee was established to provide a legal framework for members of the Energy Sector GCC and ONG SCC to engage in joint critical infrastructure protection discussions and activities, including those involved with pipeline security. Under this CIPAC committee, a Pipeline Working Group writing team was formed to develop and review applicable SSPs, including the Energy SSP and the Transportation Systems SSP. The writing team reviewed and commented on the draft Transportation Systems SSP Base Plan and drafted the Pipeline Modal Annex. The draft plans were distributed to the pipeline industry via the GCC and SCC memberships for another level of review and input before finalizing the documents.

The Transportation Security Administration (TSA) will work with its security partners in both the Transportation Systems and Energy sectors to update the Transportation Systems SSP Base Plan and Pipeline Modal Annex regularly, as called for in the NIPP and Executive Order. The updating process is a responsibility that is shared with pipeline security partners collaboratively through the GCC/SCC/CIPAC framework.

The core of the plan is a pipeline system Relative Risk Assessment and Prioritization methodology. This methodology provides a logical prioritization process to systematically list, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. By prioritization, security resources can be effectively used to manage risk mitigation in order to protect critical pipelines from terrorist threats. The methodology is based on the Transportation Systems Sector Systems-Based Risk Management (SBRM) methodology, which, in turn, is based on the risk management framework presented in the NIPP.

With a view toward this end-state, the Transportation Systems SSP and this Pipeline Modal Annex focus specifically on how the Transportation Systems Sector will continue to enhance the security of its critical infrastructure and key resources. Programs to protect the Nation's Pipeline System(s) are key to making the Nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.

Appendix 7: Select Energy-Related Cyber R&D Programs[48]

DOE is currently working with other Federal agencies and industry groups to identify and map control system projects to the needs and R&D priorities identified in the Roadmap to Secure Control Systems in the Energy Sector.[49] As of August 2006, DOE has identified more than 100 distinct projects[50] that are currently underway at the following 10 organizations:

- Pacific Northwest National Laboratory National Center for Advanced Secure Systems Research;
- DHS/National Cyber Security Division Control Systems Security Program;
- Combating Terrorism Technical Support Office/Technical Support Working Group;
- Institute for Information Infrastructure Protection;
- Trustworthy Cyber Infrastructure for the Power Grid;
- National Institute of Standards and Technology/Information Technology Laboratory Computer Security Division;
- DHS/Homeland Security Advanced Research Projects Agency Small Business and Innovative Research;
- Multi-State Information Sharing and Analysis Center;
- Digital Bond Inc./TNS Inc.; and
- DOE/OE National SCADA Test Bed Program.

National SCADA Test Bed Program R&D activities include the following projects in 2006:

- Conduct SCADA Protocol Authentication;
- Examine impacts of information technology trends on control system security (e.g., IPv6, wireless, advanced metering);
- Develop/demonstrate Virtual Control Systems Environment Tool;
- Support Trustworthy Cyber Infrastructure for the Power Grid Program (National Science Foundation);
- Work with DHS to advance Security Event Correlation technology;
- Conduct workshops on SCADA systems vulnerabilities and mitigation techniques; and

[48] Multiple technology suppliers, agencies, and industry organizations sponsor physical protection R&D projects applicable to critical infrastructure, which are also underway.

[49] January 2006, www.oe.energy.gov/DocumentsandMedia/roadmap.pdf.

[50] Source: Energetics Control Systems Project Database, under development by Energetics Incorporated, Columbia, MD.

- Continue work with the National Cyber Security Division's Process Control Systems Forum and others (e.g., NERC/Control Systems Security Working Group, AGA, API, Cybernetics).

Table A7-1: Selection of Cyber Security R&D Programs and Initiatives

Program/Initiative	Lead Organization/Participants	R&D Scope
Process Control Systems Forum	Department of Homeland Security National Cyber Security Division	International design, development, and deployment of secure control systems
Process Control Security Requirements Forum	National Institute of Standards and Technology	R&D for industrial process control systems security requirements
Institute for Information Infrastructure Protection	Dartmouth College, Department of Homeland Security Science and Technology Directorate, and National Institute of Standards and Technology	National cyber security R&D coordination program
International Electricity Infrastructure Assurance Forum	Collaboration of Australia/Canada/ New Zealand/United Kingdom/ United States stakeholders and government agencies	Electricity infrastructure protection planning
National SCADA Test Bed Program	DOE OE; Idaho, Sandia, Pacific Northwest, and Argonne National Laboratories	SCADA infrastructure testing, vulnerability assessments, and standards development
National Cyber Security Division Control Systems Security Program	Department of Homeland Security National Cyber Security Division	Provides coordination among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.
North American Electric Reliability Corporation	Nonprofit corporation consisting of eight North American regional reliability councils	Reliability standards setting and enforcement for bulk electric system
American Gas Association 12 Guidance	American Gas Association, Gas Technology Institute, and National Institute of Standards and Technology	R&D on cryptographic devices and guidelines for SCADA communication
American Petroleum Institute	Trade association for the oil and natural gas industry	Industry forum, research center, and policy input
Electric Power Research Institute	Independent, nonprofit center for public interest energy and environmental research	Technology and security research programs for the electric power industry
Instrumentation, Systems, and Automation Society ISA-SP99	The Instrumentation, Systems, and Automation Society's ISA-SP99 (Manufacturing and Control Systems Security) Committee	Development and provision of criteria for procuring and implementing secure control systems

Homeland Security

Department of Energy