Energy Sector-Specific Plan

2015

Homeland Security

Page intentionally left blank

TABLE OF CONTENTS

FIGURES AND TABLES

PREFACE

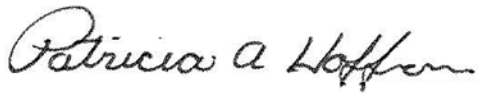
The U.S. Department of Energy (DOE), as the Sector-Specific Agency for the Energy Sector, has worked closely with government and industry partners to develop the 2015 Energy Sector-Specific Plan (SSP). DOE conducted much of this work in collaboration with the Energy Sector Coordinating Councils (SCCs) and the Energy Government Coordinating Council (GCC). The Energy SCCs represent the interests of the Electricity and Oil and Natural Gas Subsectors; the Energy GCC represents government at various levels—Federal, State, local, territorial, and tribal—as well as international partners.

The 2015 Energy SSP is closely aligned with the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) and the joint national priorities, which were developed in collaboration by representatives from all critical infrastructure sectors, including Energy. As a result, the Energy Sector has adopted the national critical infrastructure goals as the sector goals in this updated Energy SSP.

In today's fast changing world, the Nation's critical energy infrastructure continues to face new threats and challenges, as new opportunities and pathways develop over time. Some of the key tasks at hand include strengthening the resilience of supply chains, enhancing cyber and physical security, examining interdependencies within the Energy Sector and across other sectors, enhancing climate resilience, addressing the risk associated with aging infrastructure and workforce, and developing meaningful metrics to assess the sector's progress toward security and resilience. Many of these new threats and challenges will require an integrated risk-management approach and close collaboration between the government and private sector to resolve.

The revised 2015 Energy SSP highlights the maturation of the Energy Sector partnership, the sector's risk management approaches to key evolving risks and threats, as well as the continuous progress the sector has made toward a more secure and resilience critical energy infrastructure. With the NIPP 2013 and the 2015 Energy SSP as the guiding principles, Energy Sector partners will continue to work together to improve cooperation and to enhance the security and resilience of the Nation's vital energy system.

Sincerely,



Patricia Hoffman
Assistant Secretary
Office of Electricity Delivery and Energy Reliability
U.S Department of Energy

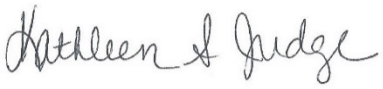
Caitlin Durkovich
Assistant Secretary
Infrastructure Protection
U.S. Department of Homeland Security

Tom Fanning
Chair, Electricity Subsector Coordinating Council

Kevin Wailes
Vice Chair, Electricity Subsector Coordinating Council

Duane Highley
Vice Chair, Electricity Subsector Coordinating Council

Brandon Martin
Chair, Oil and Natural Gas Subsector Coordinating Council



Kathy Judge
Vice Chair, Oil and Natural Gas Subsector Coordinating Council

ACRONYMS

AGA	American Gas Association
API	American Petroleum Institute
C2M2	Cybersecurity Capability Maturity Model
CFATS	Chemical Facility Anti-Terrorism Standards
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CIPC	Critical Infrastructure Protection Committee
DHS	U.S. Department of Homeland Security
DNG ISAC	Downstream Natural Gas ISAC
DOE	U.S. Department of Energy
DOT	Department of Transportation
EAGLE-I	Environment for Analysis of Geo-Located Energy Information
EEI	Edison Electric Institute
EMP	Electromagnetic pulse
EO	Executive Order
ESCC	Electricity Subsector Coordinating Council
ESF	Emergency Support Function
E-ISAC	Electricity ISAC
FACA	Federal Advisory Committee Act
FERC	Federal Energy Regulatory Commission
FOIA	Freedom of Information Act
GCC	Government Coordinating Council
GMD	Geomagnetic disturbance
HSIN	Homeland Security Information Network
IOU	Investor-owned utility
ISAC	Information Sharing and Analysis Center
IT	Information technology
LPT	Large power transformer
MTSA	Maritime Transportation Security Act
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Officials
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPC	National Petroleum Council
NRCan	Natural Resources Canada
NRF	National Response Framework
ONG ISAC	Oil and Natural Gas ISAC
PNWER	Pacific Northwest Economic Region
PPD	Presidential Policy Directive
PS Canada	Public Safety Canada
RMAG	Regional Mutual Assistance Group
RRAP	Regional Resiliency Assessment Program
R&D	Research and development
SCC	Subsector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SSA	Sector-Specific Agencies
S&T	Science and Technology Directorate

EXECUTIVE SUMMARY

The 2015 Energy Sector-Specific Plan (SSP) was developed in accordance with the *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, which guides the national effort to manage risk to the Nation's critical infrastructure. The U.S. Department of Energy (DOE), as the Sector-Specific Agency (SSA) for the Energy Sector, led the development of the 2015 Energy SSP in close collaboration with its sector partners. A myriad of Energy Sector partners exist in both private and public sectors in the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, under which the Electricity and Oil and Natural Gas Subsector Coordinating Councils (SCCs) and the Energy Government Coordinating Council (GCC) operate.

Energy Sector partners have developed a valuable and increasingly trusted partnership in the past decade, which has been the cornerstone of the Nation's integrated risk management approach to critical infrastructure security and resilience. The Energy Sector is characterized by widely-diverse infrastructure components, a multifaceted operational environment, and complex ownership and regulatory structures. Further, the Energy Sector provides one of the key lifeline-functions upon which all other critical infrastructure sectors rely—the Nation's security and economy depend on it. In turn, the Energy Sector depends on many other critical infrastructure sectors, such as transportation, information technology (IT), communications, water, and financial services. In addition, the sector faces evolving threats and risks, such as natural disaster events, cyber and physical security threats, aging/failing infrastructure, and the potential shortage of a skilled workforce.

To address these challenges, the Energy Sector has adopted national critical infrastructure security and resilience goals: assessing security risks and threats, securing critical infrastructure from all hazards, enhancing critical infrastructure resilience, sharing information to enable risk-informed decision making, and promoting learning and adaptation. In the Energy Sector, approximately 170 activities and programs support these goals and the joint national priorities; these initiatives have been developed and maintained by a wide variety of public and private organizations. Because the vast majority of energy infrastructure is owned and operated by the private sector, Energy Sector security and resilience efforts are a shared responsibility between the government and industry.

As such, research and development (R&D) efforts in the Federal Government are coordinated with the private sector counterparts as part of a robust national R&D strategy. Energy Sector's key R&D areas include reducing the social consequences of natural disasters and climate events, developing innovative tools and technologies to harden critical infrastructure, and enhancing cybersecurity capabilities to address evolving cyber threats.

Measuring progress in advancing security and resilience goals has been one of the core guiding principles of the national risk management framework for critical infrastructure. The Energy Sector's complex operating structure and the evolving threat and risk environment make it difficult to accurately assess and measure the security and reliability posture of the sector. Therefore, the Energy Sector continues to improve approaches to measure progress toward achieving the critical infrastructure security and resilience goals. This updated 2015 Energy SSP is a demonstration of the numerous achievements and the progress the sector has made toward a secure and resilient energy infrastructure.

1 INTRODUCTION

In December 2013, the U.S. Department of Homeland Security (DHS) released the updated *National Infrastructure Protection Plan 2013 (NIPP 2013)—Partnering for Critical Infrastructure Security and Resilience*, which guides the national effort to manage risk to the Nation's critical infrastructure. The NIPP 2013 represents the continuing evolution of concepts introduced in the initial version of the NIPP released in 2006 and revised in 2009, building upon the principles of Presidential Policy Directive 21 (PPD-21)—Critical Infrastructure Security and Resilience, which directs the national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. In accordance with PPD-21, the Nation's infrastructure is divided into 16 sectors, including Energy, and select Federal agencies are responsible for leading the Federal effort in each sector as the Sector-Specific Agencies (SSAs). The U.S. Department of Energy (DOE), as the Energy SSA, developed this 2015 Energy Sector-Specific Plan (SSP) in close collaboration with its government and industry partners.

The purpose of the Energy SSP is to help guide and integrate the sector's continuous effort to improve the security and resilience of its critical infrastructure and to describe how the Energy Sector contributes toward the national critical infrastructure security and resilience goals. The 2015 Energy SSP updates and augments the prior versions of the SSP in accordance with the NIPP 2013. Specifically, it includes the discussion of the many evolving risks and threats in the Energy Sector, as well as an increased emphasis on the Energy- and cross-sector interdependency issues and the integration of cyber and physical security efforts.

Critical infrastructure protection, security, and resilience are not new concepts to Energy Sector asset owners and operators. The Electricity and Oil and Natural Gas Subsectors have faced and will continue to face challenges from many types of hazards. The subsectors prepare for these challenges through an all-hazards approach that includes implementing protection measures, as well as developing, exercising, and utilizing restoration and recovery plans. Through the NIPP sector partnership, government and industry partners have established an increasingly high-level of coordination, collaboration, and cooperation, bringing together government, industry, and international partners to manage risk to critical infrastructure. This updated 2015 Energy SSP is a reflection of that valuable and growing partnership in the Energy Sector, and is a demonstration of the achievements and progress the sector has made toward a more secure and resilient energy infrastructure.

The Energy SSP is organized as shown in Table 1-1. Each section of the SSP is intended to describe the Energy Sector's efforts to achieve the critical infrastructure goals and to address specific items of "Call to Action: Steps to Advance the National Effort" as defined in the NIPP 2013 (see Table 1-1). Developed in collaboration between government and private sector partners, the "Call to Action" consists of 12 activities to guide efforts to achieve national critical infrastructure security and resilience goals.

Table 1-1: 2015 Energy SSP Section and Corresponding NIPP 2013 Call to Action

ENERGY SSP 2014 SECTION	NIPP 2013 CALL TO ACTION
1. Energy Sector Overview • Vision, Goals, and Priorities • Risk Environment in the Energy Sector	1. Establish National Focus through Joint Priority Setting 2. Determine Collective Actions through Joint Planning Efforts
2. Energy Sector Critical Infrastructure Partnership	3. Empower Local and Regional Partnerships to Build Capacity Nationally

ENERGY SSP 2014 SECTION	NIPP 2013 CALL TO ACTION
3. Sector Efforts to Achieve National Vision and Goals • Risk Management • Information Sharing and Communication • Critical Infrastructure Resilience and Preparedness	4. Leverage Incentives to Advance Security and Resilience 5. Improve Information Sharing and Apply Knowledge to Enable Risk-informed Decision Making 6. Analyze Dependencies and Interdependencies 7. Rapidly Identify, Assess, and Respond to Cascading Effects During and Following Incidents 8. Promote Infrastructure, Community, and Regional Recovery Following Incidents 9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education 12. Learn and Adapt During and After Exercises and Incidents
4. Research and Development Priorities	10. Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions
5. Measuring Progress	11. Evaluate Achievement of Goals

2 SECTOR OVERVIEW

The Energy Sector consists of widely-diverse and geographically-dispersed critical assets and systems that are often interdependent of one another. This critical infrastructure is divided into three interrelated segments or subsectors—electricity, oil, and natural gas—to include the production, refining, storage, and distribution of oil, gas, and electric power, except for hydroelectric and commercial nuclear power facilities and pipelines. The Energy Sector supplies fuels to the transportation industry, electricity to households and businesses, and other sources of energy that are integral to growth and production across the Nation. In turn, it depends on the Nation's transportation, information technology, communications, finance, water, and government infrastructures. In 2013, PPD-21 identified the Energy Sector as uniquely critical because it provides an essential function across virtually all critical infrastructure sectors.

In the United States, energy assets and critical infrastructure components are owned by private, Federal, State, and local entities, as well as certain energy consumers, such as large industries and financial institutions (often for backup power purposes). The Energy Sector is subject to regulation in various forms as they are often overseen under numerous jurisdictions. The complex operating structure, in addition to the evolving threat and risk environment, make it challenging to protect and secure the sector's critical infrastructure.

PPD-21 directed the national effort in the security and resilience of critical infrastructure to take an integrated, holistic approach to reflect the infrastructure's interconnectedness and interdependency as well as evolving risks. The NIPP 2013 and Energy Sector goals, which are discussed in the following section, reflect that approach.

2.1 Vision, Goals, and Priorities

In 2005, Energy Sector partners developed the sector vision and goals through a collaborative process between the two Subsector Coordinating Councils (SCCs) and the Government Coordinating Council (GCC). The Energy Sector vision and goals have always aligned with and supported the NIPP critical infrastructure security and resilience goals. During the NIPP 2013 development process, representatives from all critical infrastructure sectors, including Energy, closely collaborated to develop the revised national critical infrastructure goals. As a result, in 2014, the Energy Sector has adopted the national critical infrastructure goals as its sector goals. Table 2-1 provides the national vision and goals for critical infrastructure security and resilience, as well as the key priorities for the two Energy Subsectors which contribute to achieving the national goals. (See Appendix A for a cross-walk between the subsector priorities and the joint national priorities.)

Table 2-1: National and Energy Sector Critical Infrastructure Vision and Goals

VISION STATEMENT
A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

National and Energy Sector Critical Infrastructure Goals
• Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities. • Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk,

while accounting for the costs and benefits of security investments.
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services.
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.
- Promote learning and adaptation during and after exercises and incidents.

Electricity Subsector Priorities	Oil and Natural Gas Subsector Priorities
Tools and Technology—Deploying tools and technologies to enhance situational awareness and security of critical infrastructure. • Deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid. • Implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.	The Oil and Natural Gas Subsector Coordinating Council strives to provide a venue for industry owners and operators to mutually plan, implement, and execute sufficient and necessary sector-wide: security programs; procedures and processes; information exchange; accomplishment assessment; and progress to strengthen the security and resilience of its critical infrastructure. Priorities are placed in the following: • Partnership coordination; • Implementation and communication; • Identification of sector needs/gaps and/or best practices; • Information sharing; and • Business continuity.
Information Flow—Making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner. • Improving the bidirectional flow of threat information. • Coordinating with interdependent sectors.	
Incident Response—Planning and exercising coordinated responses to an attack. • Developing playbooks and capabilities to coordinate industry-government response and recovery efforts. • Ongoing assessments of equipment-sharing programs.	

2.2 Risk Environment in the Energy Sector

The risk environment of the Energy Sector continues to evolve over time as technology advances, market patterns shift, and environmental factors continue to be in a state of flux. Risk is defined as a function of consequences—human and economic, vulnerabilities, and threats.[1] Various sources continuously assess risks and threats in the Energy Sector, from government and academic institutions, to trade associations and individual companies. Considerable media attention has also been devoted to threats to energy infrastructure, including cyber and physical security threats, space weather events, and possible terrorist attacks. Once threats have been identified, consequences and vulnerabilities can be quantified to determine the cost benefits of risk mitigation measures. However, the types of threats faced by the electricity and oil and natural gas industries vary widely, as well as the meaning of "risk" as perceived by each organization. This section provides a high-level overview of the various types of risks and threats in the Energy Sector. Section 4 of this report discusses in further detail some of the key evolving threats in the sector and the various approaches Energy Sector stakeholders are taking to manage the resultant risks.

[1] The NIPP 2013 defines a risk as "the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences." See NIPP 2013, http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience (accessed December 18, 2014).

2.1.1 Electricity Subsector Risks and Threats

Many organizations conduct a wide variety of risk assessments of the Electricity Subsector. For example, the North American Electric Reliability Corporation (NERC) assesses risks in terms of the potential impact to the reliability of the bulk power system (i.e., did an event result in the loss or interruption of service to customers?), while private companies and utilities examine risks and threats as they relate to the operational and financial security of each company (i.e., could a threat negatively impact the company's financial health?). Based on a review by some of the largest U.S. electric utilities (in terms of revenue) as well as the analysis by NERC, a wide variety of issues were considered threats in the Electricity Subsector.[2] Despite the differences in what constitutes risk, the Electricity Subsector identified several issues as the key risks and threats to its infrastructure and/or continuity of business in 2012 and 2013:

- Cyber and physical security threats;
- Natural disasters and extreme weather conditions;
- Workforce capability ("aging workforce") and human errors;
- Equipment failure and aging infrastructure;
- Evolving environmental, economic, and reliability regulatory requirements; and
- Changes in the technical and operational environment, including changes in fuel supply.






2.1.2 Oil and Natural Gas Subsector Risks and Threats

The Oil and Natural Gas Subsector, particularly the oil industry, faces a diverse risk landscape due to its worldwide geographic presence, the hazardous and evolving exploration, production, and operating conditions, as well as the various domestic and in some cases foreign regulatory jurisdictions under which it operates. Based on a survey of the 100 largest U.S. exploration and production companies, the following were identified as key risks the oil and natural gas industry faced during 2012:[3]

- Natural disasters and extreme weather conditions;
- Regulatory and legislative changes—including environmental and health—as well as increased cost of compliance;
- Volatile oil and gas prices and demands;
- Operational hazards including blowouts, spills and personal injury;
- Disruption due to political instability, civil unrest, or terrorist activities;
- Transportation infrastructure constraints impacting the movement of energy resources;

[2] "ERO Reliability Risk Priorities RISC Recommendations to NERC Board of Trustees," NERC, October, 2014, http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO%20Reliability%20Risk%20Priorities%20%20RISC%20Updates%20and%20Recommendations%20-%20October%202014%20r1.pdf (accessed January 20, 2014); State of Reliability 2014, NERC, May 2014, http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf (accessed September 9, 2014).

[3] These risks were identified in the 2012 SEC 10-K filings of the largest 100 U.S. oil and natural gas exploration and production companies. See 2013 BDO Risk Factor Report for Oil and Gas Businesses, June 0213, http://www.lumsdencpa.com/documents/OilGasRiskFactorReport2013June.pdf (accessed June 3, 2014).

- Inadequate or unavailable insurance coverage;
- Aging infrastructure and workforce; and
- Cybersecurity risks, including insider threats.[4]

[4] "Sector Risk Snapshot," DHS, May 2014, https://www.hsdl.org/?view&did=754033 (accessed May 21, 2015).

3 ENERGY SECTOR CRITICAL INFRASTRUCTURE PARTNERSHIP

The development of the public-private partnership has been the most valuable aspect of the ongoing critical infrastructure security and resilience efforts in the Energy Sector. It is only through a true partnership that the Energy Sector is able to realize its security and resilience goals. Therefore, the Energy Sector, with a myriad of voluntary representatives made up of asset owners and operators, academia and research partners, international partners, as well as Federal, State, and local government officials, has placed a considerable effort into fostering and maintaining trusted partnerships.

Voluntary participation and partnerships help facilitate the useful exchange of security-related information and maximize the effectiveness of infrastructure protection and resilience efforts. They also promote the cooperation necessary to speed restoration and recovery with activities such as equipment and personnel sharing. The development and implementation of the Energy SSP has relied upon this partnership, and the Energy SSP helps guide the sector's continuing effort to improve security and resilience of the critical infrastructure. This section describes the public-private partnership that is the cornerstone of the Energy Sector's critical infrastructure security and resilience efforts.

3.1 Energy Sector Partners

In the Energy Sector, the core of critical infrastructure partners consists of two SCCs and the GCC as shown in figure 3-1. The Electricity SCC (ESCC) and the Oil and Natural Gas (ONG) SCC represent the interests of their respective industries. The Energy GCC, co-chaired by DOE and DHS, represents many levels of the government—Federal and State, Local, Tribal, and Territorial (SLTT)—and international partners that are concerned with the Energy Sector.

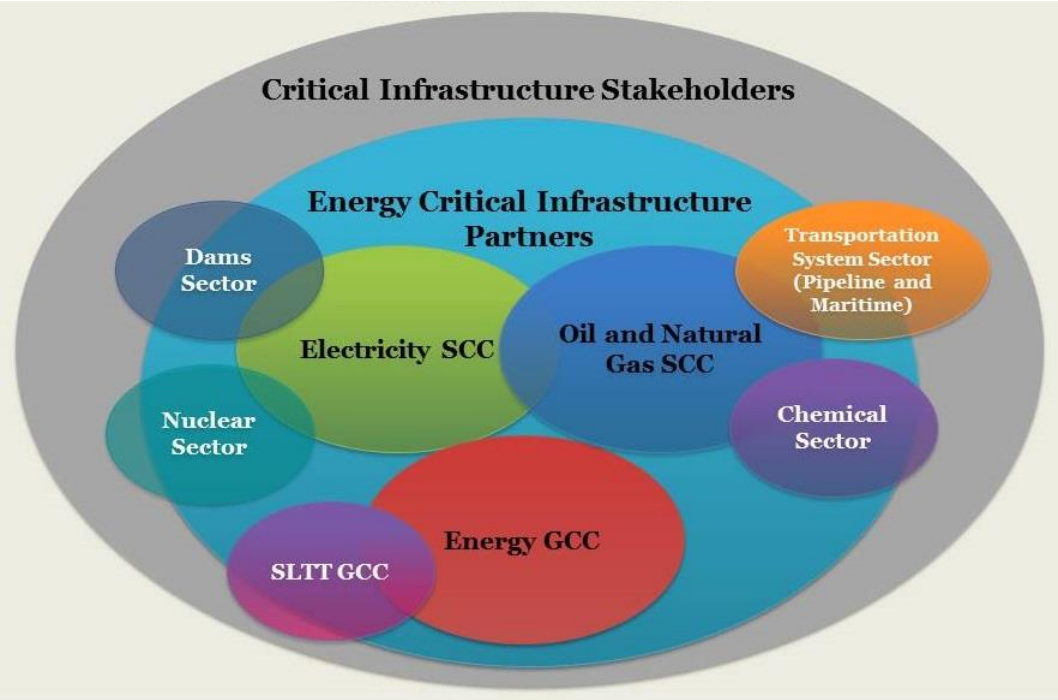
As defined in the NIPP, the SCCs are created by owners and operators and are self-organized, self-run, and self-governed, with a leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.[5]

The SCCs, GCC, and associated working groups operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and government coordination.[6] CIPAC exempts partnership meetings from the Federal Advisory Committee Act (FACA), allowing the public-private critical infrastructure community to engage in open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

[5] NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, DHS, January 2014, http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience (accessed September 8, 2014).
[6] "Charter of the Critical Infrastructure Partnership Advisory Council CIPAC)," DHS, http://www.dhs.gov/critical-infrastructure-partnership-advisory-council (accessed September 18, 2014).

Figure 3-1 illustrates the intersection of the many Energy Sector stakeholders that collaborate within the critical energy infrastructure community and other critical infrastructure sectors that are also stakeholders in the Energy Sector. The full list of SCC and GCC members under the CIPAC framework is updated quarterly and available at DHS.[7]

Figure 3-1: Critical Infrastructure Stakeholders in the Energy Sector



3.1.1 Electricity Subsector Coordinating Council

The ESCC serves as the principal liaison between the Federal Government and the Electricity Subsector with the mission of coordinating efforts to prepare for and respond to national-level disasters or threats to critical infrastructure.[8] The ESCC includes corporate CEOs and trade association leaders representing all segments of industry, including investor-owned, municipal, and cooperative entities. The ESCC coordinates with senior government officials of the Energy GCC focusing primarily on three areas: tools and technologies, information flow, and incident response.

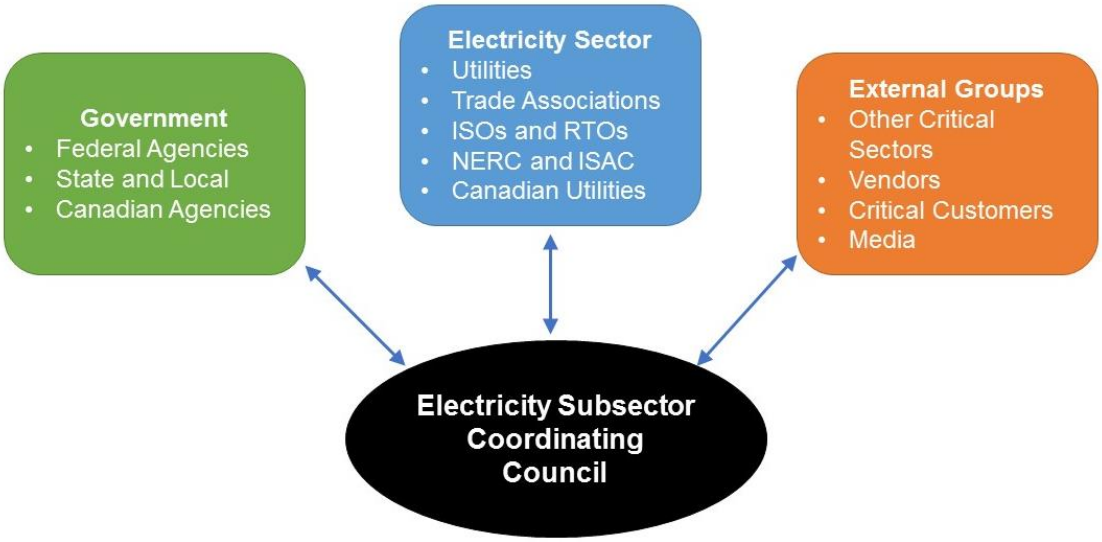
The ESCC clearly identifies the key players, areas of focus, coordination of responsibilities (see figure 3-2), as well as the organizational structure. The ESCC stated that the "[c]oordination among senior government and industry executives helps to ensure an effective response, appropriate prioritization and allocation of resources, and support for […] procedures during an incident."[9]

In addition to the ESCC, NERC's Critical Infrastructure Protection Committee (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 cybersecurity, physical security, and operational security. Both DOE and DHS participate in the CIPC, allowing it to serve as a mechanism within the Electricity Subsector for

[7] "Critical Infrastructure Partnership Advisory Council Sector Charters and Membership," DHS, http://www.dhs.gov/cipac-sector-charters-and-membership (accessed October 15, 2014).
[8] Electricity Subsector Coordinating Council (ESCC) Brochure, February 2014, http://www.publicpower.org/files/PDFs/ESCC%20Overview%20Brochure%20-%20February%202014.pdf (accessed September 17, 2014).
[9] *Ibid.*

collaboration between the government and the industry. In addition, industry trade associations play an important role in coordination and collaboration, including the Edison Electric Institute (EEI), the National Rural Electric Cooperative Association, and the American Public Power Association, as they represent the interests of the Electricity Subsector.

Figure 3-2: ESCC Coordination of Responsibilities



Source: ESCC

3.1.2 Oil and Natural Gas Subsector Coordinating Council

The ONG SCC is the primary conduit for industry and government for national level coordination of protection and resilience activities in the Oil and Natural Gas Subsector. Through the ONG SCC, oil and natural gas industry stakeholders have maintained longstanding partnerships with many levels of government to coordinate the infrastructure security and resilience efforts associated with all hazards. The ONG SCC seeks to provide a venue for industry owners and operators to mutually plan, implement, and execute sufficient and necessary sector-wide security programs, procedures and processes, information exchange, accomplishment assessment, and progress toward securing the sector's critical infrastructure. The ONG SCC represents the interests of oil and natural gas infrastructure owners and operators with representatives from more than 20 industry trade organizations. The council chairperson and leadership are the primary contacts for the SCC's government counterparts. The members of the ONG SCC also work on transportation sector pipeline efforts through the Pipeline Working Group that serves as the Pipeline Modal SCC for the Transportation Systems Sector.

The ONG SCC develops a strategic plan for the sector outlining its priorities and participates in the development of policy related to critical infrastructure security and resilience. For example, the Energy SSA and ONG SCC have collaborated with the Chemical SSA and Chemical SCC in the development of cross-sector metrics and the implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) and Maritime Transportation Security Act (MTSA), among other activities. Also, the ONG SCC facilitated the participation of industry partners and their government counterparts in a National Petroleum Council (NPC) study to provide input into future policy development.

Completed in December 2014, the NPC study provides advice on how the oil and natural gas industry and government at many levels can better prepare for and respond to emergencies. Specifically, the NPC study addressed: 1) Actions by government and industry to improve their interactions to prepare for and respond to emergencies that can disrupt oil and natural gas supplies and other dependent critical services, 2) Data, technologies, or other capabilities to improve situation assessment, 3) Legal, procedural, or physical challenges to emergency response and restoration, and strategies to improve

emergency preparedness and resiliency, and 4) Strategies to address interdependencies among oil and natural gas and other critical infrastructure.[10]

Similar to the Electricity Subsector, the ONG SCC is composed of various oil and natural gas industry trade associations who play an integral role in coordination and collaboration with government, including the American Gas Association (AGA), the American Petroleum Institute (API), the Interstate Natural Gas Association of America, the International Liquid Terminals Association, and the American Fuel and Petrochemical Manufacturers Association. In 2013, API, with support from all these associations, developed the *Oil and Natural Gas Industry Preparedness Handbook*, a "strategy document to ensure that roles, responsibilities and needs are clearly identified prior to any events that may affect the integrity of oil and natural gas systems."[11]

3.1.3 Energy Government Coordinating Council

The government counterpart for the SCCs is the Energy GCC, which is co-chaired by DOE and DHS, and is composed of representatives across many levels of the government—Federal and SLTT—and international partners that are concerned with the security of the Energy Sector.[12] The Energy GCC includes representatives from the SLTT GCC, which brings together experts from a wide range of professional disciplines related to critical infrastructure protection from all levels of government. In addition, representatives from Natural Resource Canada (NRCan) and Public Safety Canada (PS Canada) are members of the Energy GCC. The members of the Energy GCC are also engaged in other critical infrastructure sectors' security and resilience efforts, including pipeline, maritime, chemical, and dams.

The Energy GCC plays a critical role in implementing the Energy SSP. Through the NIPP partnership model, the Energy GCC maximizes efficiency by collaborating with energy and other critical infrastructure sector partners at various levels. Together with Energy SCCs, the GCC helps develop and prioritize various security programs and initiatives supporting the NIPP and the Energy SSP.

Energy SSA Roles and Responsibilities

As the Energy SSA, DOE works at many levels of 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 and reliability. In addition, numerous working groups exist between government and industry, as well as through industry associations at the national, regional, State, and local levels.

DOE and the sector partners have and will continue to coordinate with other Federal agencies that have energy-related response and security responsibilities and programs. DOE will continue to support effective practices and partner, where practical, with these agencies in implementing security and resilience programs. The responsibilities of various government agencies under the National Response Framework (NRF) 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 the DHS Office of Infrastructure Protection, the Federal Emergency Management Agency, Environmental Protection Agency, Department of

[10] "Enhancing Emergency Preparedness for Natural Disasters: Government and Oil and Natural Gas Industry Actions to Prepare, Respond, and Recover," National Petroleum Council, December 18, 2014, http://www.npc.org/reports/NPC_EmPrep_Report_2014-12-18.pdf (accessed September 18, 2014).
[11] "Oil and Natural Gas Industry Preparedness Handbook," API, October 2013, http://www.api.org/~/media/Files/Policy/Safety/ONG-Industry-Preparedness-Handbook-v2.pdf (accessed September 18, 2014).
[12] DHS, 2009 National Infrastructure Protection Plan, section 4.1.2.3, p. 52 http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (March 2009).

Transportation (DOT), State and local government, utilities, and others, as they perform DOE's Emergency Support Function-12 (ESF-12) responsibilities.[13] DOE has longstanding relationships with many Federal agencies to help fulfill its mission to provide safe and secure energy supplies.

State, Local, Tribal, and Territorial Agencies

SLTT governments are crucial stakeholders in providing a secure and reliable energy infrastructure for the Nation. They are responsible for emergency planning and response, developing energy security and reliability policies and practices, and facilitating Energy Sector protection activities. In times of crisis, citizens turn to these organizations, which play a significant role in preparing for and responding to energy supply events and mitigating the impacts of emergencies that do arise.

State and local governments are required under Federal homeland security funding guidance to implement the NIPP, as well as the NRF and National Incident Management System. As State and local governments develop their critical infrastructure plans, each Governor has designated a State administrative agency to support the development of homeland security strategies, implement strategic goals and objectives, and administer Federal preparedness assistance. The National Association of State Energy Officials (NASEO), in collaboration with the National Association of Regulatory Utility Commissioners (NARUC), has produced Energy Assurance Guidelines that outline States' overall role in energy assurance.[14] This role includes operating within the Federal ESF 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 continue to work with DOE to conduct multi-State and regional exercises and training sessions on energy emergency preparedness, response, and key Critical Infrastructure Protection (CIP) issues, as well as provide technical assistance to States to update their energy assurance plans.

Due to State responsibilities for public utilities that provide a direct service to their citizens, States are particularly concerned with programs related to the sharing of information with other critical sectors. Public utility commissions also support emergency management and response activities during events that affect utility facilities, systems, and services. DOE continues to work with SLTT governments to identify gaps in meeting sector goals, improve existing State-focused programs, and implement new programs to eliminate identified vulnerabilities.

[13] See Section 3.4 Critical Infrastructure Resilience and Preparedness for more information on ESF-12.
[14] Energy Assurance Guidelines, National Association of State Energy Officials, www.naseo.org/eaguidelines (accessed October 15, 2015).

Executive Collaboration for the Nation's Strategic Infrastructure
National Infrastructure Advisory Council (NIAC), March 20, 2015

NIAC's March 2015 report highlighted the need for engagement of senior executive leadership in the public-private partnership to advance the mission for critical infrastructure resilience. In this report, NIAC proposed establishing two CEO-level national frameworks—one for engagement and one for communication—to engender engagement of CEOs or equivalent decision-makers and their counterparts in the Federal Government.

The purpose of the Engagement Framework is to identify and prioritize national critical infrastructure security and resilience issues affecting national and economic security, as well as the challenges in addressing those priorities, and to develop mutual strategies and policies, including roles and responsibilities, and to jointly take action to empower achievement of measurable results. For the Engagement Framework, NIAC recommended the establishment of the Strategic Infrastructure Executive Council under CIPAC, as well as a permanent budget line to provide permanent staff, analytic resources, and administrative support to facilitate that council. For any proposed engagement, NIAC further recommended that DHS work with the SSAs and the National Security Council to identify, clarify, and articulate national priorities and value propositions.

For the Communication Framework, NIAC recommended tailoring of the messaging—both content and format—of communication to be relevant to the CEO's responsibilities and be as efficient as possible, and to utilize established, CEO-credible or "trusted" channels or venues for transmittal of communication.

Finally, NIAC recognized that certain critical infrastructure sectors may have different priorities, and that the CEO engagement model does not work for all sectors. The NIAC report is available at http://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf

4 SECTOR EFFORTS TO ACHIEVE NATIONAL VISION AND GOALS

In the Energy Sector, critical infrastructure security and resilience goals and priorities are developed and achieved through a collaborative effort between the industry and the government. As discussed in Section 2, these goals include assessing security risks and threats, securing critical infrastructure from all hazards, enhancing critical infrastructure resilience, sharing information, and promoting learning and adaptation. There are numerous activities and programs that support these goals, developed and maintained by a wide variety of public and private organizations. Because the vast majority of energy infrastructure is owned and operated by the private sector, the Energy Sector security and resilience efforts are a shared responsibility between the public and private sectors. This section highlights some of the approaches and efforts that are underway in the Energy Sector to help achieve the national critical infrastructure security and resilience goals.

4.1 Risk Management

The Energy Sector has extensive, in-depth experience in risk management, to enhance the security posture of its critical infrastructure that consists of highly diverse assets, systems, functions, and networks. To address such diverse assets that span the Nation, various risk assessment methods are applied—many of which are tailored to a specific segment of the sector (e.g., electricity, oil, natural gas, or their system components). The industry has responded to the increased need for enterprise-level security efforts and business continuity plans, and continues 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. In addition, the Energy Sector has methodologies that are being used to assess risks at the system and the sector levels, as well as some with broader applicability that extends across multiple critical infrastructure sectors. This section briefly discusses the various risk assessment approaches that exist in the Energy Sector, as well as some of the key evolving risks facing the sector and the risk management efforts to manage those risks.

4.1.1 Risk Assessment

A broad range of methods are used by the Energy Sector to assess risk, which include 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 infrastructure protection and resilience investments based on risk. It has also highlighted the importance of interdependencies within the sector as well as across other critical infrastructure sectors.

Goal:

"Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities."

It is not only a common business practice, but also a mission of individual owners and operators to ensure the security and protection of their own assets. For that reason, as part of everyday operation, they develop and apply facility and system risk assessment methodologies. Asset owners and operators also prioritize their assets for protection and plan for possible restoration and recovery from anticipated threats. In addition to the owners and operators' risk management approaches, the Energy Sector employs risk assessment

methods developed by professional and trade associations, academic institutions, research centers, and Federal and SLTT governments.

DOE, in cooperation with industry partners, has undertaken programs to assess the risks of key energy infrastructure assets and to help provide technology, tools, and expertise to other Federal and SLTT organizations and the private sector. These programs are designed to assist all entities within the energy infrastructure in securing systems against physical and cyber attacks. DOE, in cooperation with DHS and industry partners continue working to:

- Strengthen the energy industry's integrated cyber-physical capabilities;
- Enhance energy infrastructure reliability and cybersecurity solutions development;
- Continue efforts to identify and prepare for future challenges to grid reliability;
- Assist other critical infrastructure sectors' efforts to analyze and address their dependence on Energy Sector's lifeline function; and
- Stimulate support and interaction with key infrastructure suppliers and vendors.

4.1.2 Energy Sector Risks

The Energy Sector faces a wide variety of risks that are evolving and may be difficult to assess or quantify due to a high level of uncertainty about the frequency or severity of the event. Some of these risks include cyber and physical security threats, space weather events, aging infrastructure and an aging workforce, as well as climate change. The ability of energy infrastructure to continue to adapt to these threats is critical, especially during recovery from a disaster, because many critical infrastructure and essential functions—including hospitals, water and wastewater systems, transportation, and telecommunication—depend on the reliable supply and delivery of electricity and other fuels to operate. As such, Energy Sector partners have undertaken many initiatives to address these evolving risks as discussed in this section.

Goal:

"Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments."

Cybersecurity

Cybersecurity is a growing and evolving security challenge for the Energy Sector and more generally for the U.S. economy. Because of the shared responsibility to secure North America's energy delivery systems against cyber threats, a common vision and framework is needed to guide the public-private partnerships. Both the electricity and the oil and natural gas industries have initiated enhanced approaches to plan for and counter cybersecurity threats to energy infrastructure operations.

In February 2013, the President signed Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," setting forth policies to address evolving cyber threats. Specifically, EO 13636 directed the National Institute of Standards and Technology (NIST) to work with stakeholders to develop a cybersecurity framework. To facilitate the Energy Sector's implementation of the NIST Cybersecurity Framework, DOE and industry partners collaborated to develop the Energy Sector Cybersecurity Framework Implementation Guidance, which relies on existing sector-specific standards, tools, and processes to help industry characterize, enhance, and communicate their cybersecurity posture using the NIST Cybersecurity Framework.

DOE, in collaboration with industry partners, developed the Cybersecurity Capability Maturity Model (C2M2) program in 2011. The C2M2 program is a public-private partnership effort to improve Energy Sector cybersecurity capabilities and to understand the cybersecurity posture of the industry. With support from the White House and in cooperation with DHS and industry experts, DOE developed two distinct C2M2s in 2014—one for the Electricity Subsector and another for the Oil and Natural Gas Subsector—to help organizations evaluate, prioritize, and improve cybersecurity capabilities.[15]

DOE also works with industry to develop new cybersecurity solutions for energy delivery systems through an integrated planning and research and development (R&D) effort. DOE's Cybersecurity for Energy Delivery Systems is one such program, which emphasizes collaboration among the government, industry, universities, national laboratories, and end users to advance R&D in cybersecurity.[16] The aim of the program is to reduce the risk of energy disruptions due to cyber incidents as well as survive an intentional cyber assault with no loss of critical function. This program is helping to increase the security of energy delivery systems around the country.

A comprehensive risk management approach can provide a means to develop a cybersecurity strategy tailored to the unique requirements of each asset owner. The U.S. government and regulatory authorities are exploring options for incentives such as grants, liability limitation, cybersecurity insurance, public recognition, and rate recovery to encourage the adoption of best practices across the industry. The Federal Government will need to engage owners and operators in the identification of incentives that provide the greatest value.

In addition to government programs, various industry partners, including trade associations, have been carrying out numerous cybersecurity related activities. They include the establishment of three Information Sharing and Analysis Centers (ISACs),[17] and efforts under various cyber working groups through trade associations, the development of enterprise-wide cybersecurity guidance, as well as the development of the NERC CIP Reliability Standards.

Physical Security and Resilience

Recent instances of extreme weather and grid sabotage have underscored the importance of physical security and resilience of the energy infrastructure. Specifically, in summer 2012, severe wind and thunderstorms known as a derecho devastated power systems in the Midwest and Mid-Atlantic, causing blackouts for five million electric customers from Illinois to New Jersey. The derecho was followed by Hurricane Sandy in October 2012, which cut power to more than 10 million homes and businesses in 17 States along the East Coast, in some cases for weeks.[18] This event required a national response to get the grid back up and running. (See the next section for a further discussion on the risk of natural disasters and climate change.)

Another incident occurred in April 2013 during which attackers used high-powered rifles to destroy a number of power transformers at a transmission substation in California. Although the targeted utility avoided a blackout, the incident incurred more than $15 million in damages that required nearly a month to repair.[19]

---

[15] Electricity Subsector Cybersecurity Capability Maturity Model, http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf; Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model http://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf (accessed June 5, 2014).
[16] "Cybersecurity for Energy Delivery Systems program," DOE, http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity (accessed January 20, 2015).
[17] See Section 4.3 Information Sharing for more information on the ISACs.
[18] Binz, R. et. al., "Practicing Risk-Aware Electricity Regulation: 2014 Update," Ceres, November 2014, http://www.ceres.org/resources/reports/practicing-risk-aware-electricity-regulation-2014-update (accessed December 18, 2014).
[19] *Ibid.*

The Energy Sector continues to face physical security risks, including attacks to the physical electric infrastructure such as Large Power Transformers (LPTs)[20] and the infrastructure that control cyber components. Physical attacks to the grid can "adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures."[21] The United States depends on various technologies—electricity, satellite, GPS, telecommunications, and the Internet—that are interdependent of one another for many essential functions. The failure of U.S. power infrastructure, specifically, LPTs could present vulnerability to the electric grid. Currently, the United States heavily depends on oversea manufacturers for its demand for LPTs; supply and procurement of LPTs can be challenging, as it can take more than 12 months to replace an LPT due to its long and complex procurement process.

In recognition of the importance of the electric infrastructure, there are various ongoing efforts to enhance the electric grid security and resilience. They include the development of the NERC Reliability Standards pertaining to physical security and geomagnetic disturbances (GMD) impacts,[22] industry-led electrical equipment sharing programs,[23] the analysis of power transformer manufacturing and supply chain issues,[24] DOE's electric substation security awareness campaign, and continuous research and development of hardening options by manufacturers, including recovery power transformers.[25]

Natural Disasters and Climate Resilience

Weather-related events, including lightning and storms, have historically been the biggest threat to the critical energy infrastructure. The Energy Sector will be impacted by weather patterns that may affect the frequency and severity of natural disasters, including hurricanes, floods, earthquakes, tornados and others. Such events may adversely impact the operation of power plants, the generation and the delivery of fuels and electric power, and the reliability of pipelines and electricity grids.

Energy production and distribution systems are designed to respond to weather variability such as daily changes in temperature that affect the load or rapid changes in renewable resource availability that affect the supply. These short-term fluctuations are managed by designing redundancy in the energy systems and using tools to predict, evaluate, and optimize response strategies in the near term. However, infrastructure is vulnerable to direct impacts from severe weather events. Across the nation, as in every other corner of the world, natural disasters have the potential to significantly impact the short-term domestic energy supplies.

Consequently, Federal and SLTT governments and the private sector are exploring measures to enhance resilience against natural hazards. The government efforts to strengthen climate resilience are pursued in the Energy Sector as directed in Executive Order 13653, signed by the President in November 2013. Executive Order 13653, "Preparing the United States for the Impacts of Climate Change," established an interagency Council on Climate Preparedness and Resilience and directed Federal agencies to promote: (1) engaged and strong partnerships and information sharing at all levels of government; (2) risk-informed decision-making and the tools to facilitate it; (3) adaptive learning, in which experiences

[20] Large power transformers (LPTs) are broadly used to describe a power transformer with a maximum capacity rating greater than or equal to 100 MVA. See http://energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf (accessed September 15, 2014).
[21] Order RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166, March 7, 2014, http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf (accessed September 17, 2014).
[22] Project 2014-04 Physical Security, http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx; "Project 2013-03 Geomagnetic Disturbance Mitigation," NERC, http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx (accessed July 14, 2014).
[23] http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx and http://www.nerc.com/pa/RAPA/sed/Pages/Spare-Equipment-Database-(SED).aspx (accessed July 14, 2014).
[24] "Large Power Transformers and the U.S. Electric Grid," DOE, April 2014, http://www.energy.gov/sites/prod/files/2014/04/f15/LPTStudyUpdate-040914.pdf (accessed July 9, 2014)
[25] For more information about Recovery Transformers, see: http://www.dhs.gov/files/programs/st-snapshots-prototyping-replacement-ehv-transformers.shtm (accessed July 8, 2014).

serve as opportunities to inform and adjust future actions; and (4) preparedness planning.[26] DOE, as a member of the interagency Council on Climate Preparedness and Resilience, is responsible for carrying out these initiatives for the Energy Sector. Further, the National Oceanic and Atmospheric Administration launched a new website, "climate.gov," to "promote public understanding of climate science and climate-related events . . . and to provide climate-related support to the private sector and the Nation's economy."[27]

Aging Infrastructure and the Need for Infrastructure Investment

According to a DHS study, "[s]ignificant numbers of critical infrastructure assets in the United States have reached or are approaching the end of their designed life span. Although an infrastructure does not fail because of advanced age alone, aging assets may have degraded performance or functional obsolescence that increases the risk of failure."[28] Therefore, energy infrastructure must continue to be developed, constructed, operated, and maintained to meet future demands and overcome evolving threats and other challenges.

In conducting a comprehensive long-term assessment of the assets and systems as well as for future investments, Energy Sector owners and operators are increasingly considering building resilience into new infrastructure through a variety of approaches. The energy industry works with policymakers and regulators to support effective policies to address the risks of developing, constructing, operating, and maintaining infrastructure, as well as the challenges of raising needed capital to fund transmission and distribution development.

The National Academy of Engineering cites electrification—generation, transmission, and distribution of electricity—as the most important engineering achievement of the 20th Century.[29] However, the 21st Century brings new challenges and opportunities. Improvements to the electric grid continue to be made to address the Nation's needs—modernizing infrastructure through technological innovations, improving resilience, implementing public policy requirements, addressing environmental concerns, responding to emerging physical and cyber threats, and meeting changing customer expectations.

Investment risk in the electric grid, particularly for transmission infrastructure, can be significant. Transmission projects typically require long lead times for planning, siting, and permitting and involve stakeholder processes, public policy, and construction challenges. Despite these risks, the industry continues to invest in infrastructure. For example, in 2012, investor-owned electric utilities and stand-alone transmission companies invested $35 billion in transmission and distribution infrastructure.[30] This represented a five percent increase in distribution and a 24 percent increase in transmission investment over 2011.[31] The electric power industry is also "investing more than $90 billion each year, on

[26] "Executive Order -- Preparing the United States for the Impacts of Climate Change," the White House, November 1, 2013, http://www.whitehouse.gov/the-press-office/2013/11/01/executive-order-preparing-united-states-impacts-climate-change (accessed July 7, 2014).
[27] NOAA Climate.gov, http://climate.gov/ (accessed September 11, 2014).
[28] "National Risk Estimate: Risks to Physical Infrastructure from Aging and Failing (NRE)," DHS Office of Cyber and Infrastructure Analysis, December 2014.
[29] "The Greatest Engineering Achievements," National Academy of Engineering, http://www.greatachievements.org/ (accessed September 22, 2014).
[30] "EEI Survey Shows Electric Power Industry Made Record Levels of Investment in Transmission and Distribution," Edison Electric Institute, December 18, 2013, http://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/EEI%20Survey%20Shows%20Electric%20Power%20Industry%20Made%20Record%20Levels%20of%20Investment%20in%20Transmission%20and%20Distribution.aspx, (accessed January 20, 2015).
[31] *Ibid.*

average, to transition to a cleaner generating fleet and to enhance the electric power grid to meet the needs of our 21st-century digital economy."[32]

There has been an unprecedented level of development of unconventional natural gas and crude oil in North America, particularly from shale formations, shifting the flow of oil and natural gas. Insufficient or aging infrastructure has a potential to constrain market growth and strand supplies, potentially leading to increased vulnerability.[33] Resilience is an integral element of the natural gas industry's critical infrastructure security and resilience mission. Resilience is bolstered by multiple layers of safety and reliability mechanisms to reduce the magnitude and duration of disruptive events and to ensure sufficient backup coverage. Furthermore, redundancies, interconnects, and alternative routes effectively move products around the incident, preventing major disruptions.

As with any sector, the Energy Sector is experiencing new and innovative approaches to deliver electricity more efficiently, safely, and reliably, through research done at the national laboratories, Electric Power Research Institute, and other industry research groups. In conducting a comprehensive long-term assessment of their assets and systems as well as for future investments, Energy Sector owners and operators have built and continue to build resilience into their infrastructure through a variety of approaches.

Workforce Development

The growing potential gap in available skilled labor to replace the retiring workforce has been a concern in the Energy Sector for some time. As energy demand and infrastructure needs continue to evolve, the loss of industry workers due to retirement and the accompanying loss of skills, experience, and knowledge base poses an increasing need for a new skilled workforce. More than half of utility workers will be eligible to retire in the next several years, taking years of experience and expertise with them, yet attracting a new generation of workers in the utility workforce is challenging.

Both the Electricity and Oil and Natural Gas Subsectors face the challenge of providing the workforce and expertise needed to meet future energy needs. Detailed and expansive planning on how to educate and train the next generation of workers is essential, and the Energy Sector stakeholders have been undertaking proactive measures to address the prospective shortage of trained personnel in the industry. Ongoing efforts include Industry programs and partnerships,[34] DOE funding provided for workforce training in the Electricity Subsector,[35] industry-wide workshops and conferences,[36] a joint electricity and natural gas workforce management initiative,[37] and State- and enterprise-specific assessments.[38]

[32] "EEI Statement on EPA's Proposed Guidelines for Greenhouse Gas Emissions from Existing Generation Sources," Edison Electric Institute, June 2, 2014, http://www.eei.org/resourcesandmedia/newsroom/Pages/Press%20Releases/EEI%20Statement%20on%20EPA%E2%80%99s%20Proposed%20Guidelines%20for%20Greenhouse%20Gas%20Emissions%20from%20Existing%20Generation%20Sources.aspx (accessed January 20, 2015).
[33] "North American Midstream Infrastructure through 2035: Capitalizing on Our Energy Abundance," INGAA, March 18, 2014, http://www.ingaa.org/File.aspx?id=21498 (accessed July 22, 2014).
[34] For example, the Center for Energy Workforce Development, http://www.eei.org/about/affiliates/cewd/Pages/default.aspx
[35] "Workforce Training for the Electric Power Sector: Awards," DOE, http://energy.gov/oe/downloads/workforce-training-electric-power-sector-awards (accessed July 8, 2014).
[36] Utility Aging Workforce Conference, April 2014, http://www.euci.com/pdf/0414-aging.pdf (accessed July 8, 2014).
[37] Center for Energy Workforce Development (CEWD), http://www.cewd.org/ (accessed September 11, 2014).
[38] See "Review of the Aging Workforce of the Florida Electric Industry," Florida Public Service Commission, June 2011, http://www.psc.state.fl.us/publications/pdf/electricgas/Review_Fl_Electric_Industry.pdf; "State of the Energy Workforce," CEWD,

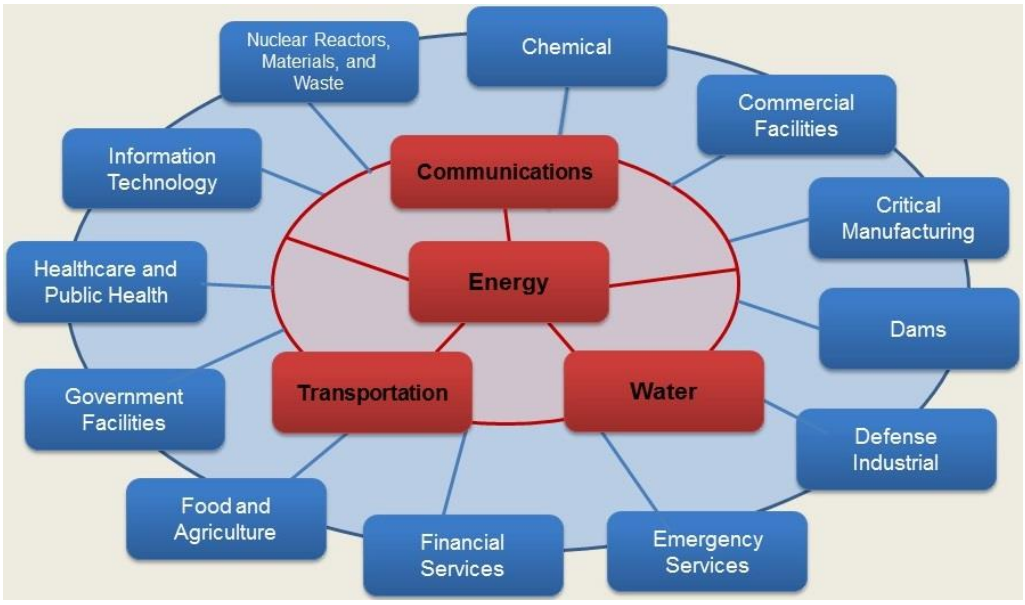
4.2 Interdependency and Coordination

The Energy Sector depends on other sectors to help provide its services, and it supplies energy services upon which all other sectors depend. Interdependencies also exist within the sector itself. A comprehensive understanding of such interdependencies enables the sector to mitigate potential vulnerabilities and helps ensure that the Nation's economy continues to deliver goods and services during extraordinary events. DOE, as the Energy SSA, continues to work with its sector partners to help identify program gaps and improve the effectiveness of sector infrastructure and resilience programs. This section provides a brief discussion of the key dependencies and interdependencies within the Energy Sector, as well as across various critical infrastructure sectors, and what efforts are underway to better understand and mitigate potential impacts.

4.2.1 Cross Sector Interdependency

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. The energy infrastructure provides essential fuel to all critical infrastructure sectors, and without energy, none of them can operate properly. Thus the Energy Sector serves one of the four lifeline functions, which means that its reliable operation is so critical that a disruption or loss of energy function will directly affect the security and resilience of other critical infrastructure sectors. In turn, the Energy Sector depends on many other critical infrastructure sectors, such as transportation, information technology (IT), communications, water, financial services, and government facilities. A disruption in a single facility of capability can generate disturbances within other infrastructure or sectors and over long distances. A series of related interconnections can extend or amplify the effects of a disruption. Figure 4-1 is a simplified illustration of the interdependencies among 16 critical infrastructure sectors, including the four critical lifeline sectors—Communications, Energy, Transportation Systems, and Water—that provide lifeline functions to all critical infrastructure sectors.

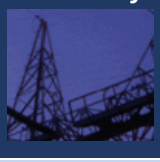
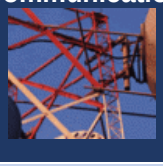
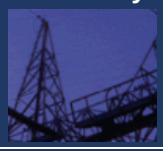
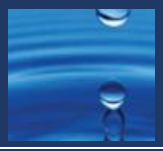
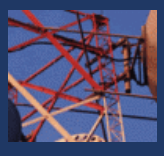
Figure 4-1: Critical Infrastructure Interdependencies



http://www.pge.com/includes/docs/pdfs/about/careers/powerpathway/newseventsmedia/CEWD_State_of_Energy_Workforce_Report.pdf (accessed July 8, 2014).

Table 4-1 provides a high level overview of the interdependency among the lifeline functions.[39] As shown in this table, the Electricity and Oil and Natural Gas Subsectors provide essential power and fuels to Communication, Transportation, and Water Sectors, and in return both subsectors rely on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication).

Table 4-1: Overview of Generic Interdependency among Critical Infrastructure Sectors

(Sub)sector Generating the Service	(Sub)sector Receiving the Service				
	ONG 	**Electricity** 	**Transportation** 	**Water** 	**Communication** 
ONG 		Fuel to operate power plant motors and generators	Fuel to operate transport vehicles	Fuel to operate pumps and treatment	Fuel to maintain temperatures for equipment; fuel for backup power
Electricity 	Electricity for extraction and transport (pumps, generators)		Power for overhead transit lines	Electric power to operate pumps and treatment	Energy to run cell towers and other transmission equipment
Transportation 	Delivery of supplies and workers	Delivery of supplies and workers		Delivery of supplies and workers	Delivery of supplies and workers
Water 	Production water	Cooling and production water	Water for vehicular operation; cleaning		Water for equipment and cleaning
Communication 	Breakage and leak detection and remote control of operations	Detection and maintenance of operations and electric transmission	Identification and location of disabled vehicles, rails and roads; the provision of user service information	Detection and control of water supply and quality	

Source: IEEE

Over time, cyber/IT dependencies have increased dramatically. For example, electricity and natural gas suppliers rely heavily on data collection systems to ensure accurate billing. Energy control systems and the information and communications technologies on which they rely play a key role in the North American energy infrastructure. These cyber/IT components are essential in monitoring and controlling the production and distribution of energy. They have helped to create the highly reliable and flexible energy infrastructure in the United States; however, the reliance of energy infrastructure on cyber infrastructure can also present vulnerability.

[39] Zimmerman, R. and Restrepo, C., "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction," 2009 IEEE International Conference on Technologies for Homeland Security, http://research.create.usc.edu/cgi/viewcontent.cgi?article=1146&context=nonpublished_reports (accessed September 17, 2014).

To better understand and mitigate potential impacts of cross-sector interdependencies, various regional and local exercises and coordinating activities are underway, including the Regional Resiliency Assessment Program (RRAP)[40] and a 2011 study by DOE and DHS examining the interdependency between the Dams and Energy Sectors.[41] During Hurricane Sandy, the Electricity Subsector relied on the fuel to power their tools and equipment, transportation to move mutual aid crews and equipment to help support the disaster areas, and communications to communicate restoration efforts in an efficient and effective manner.

4.2.2 Electricity and Natural Gas Interdependency

In addition to cross-sector interdependencies, substantial interdependencies exist within the Energy Sector, including between electricity and natural gas infrastructure. With an abundant production and a declining price, natural gas is being used more heavily in electricity generation, yet there are various reliability issues, including constrained infrastructure capacity to deliver natural gas supplies to power generators in certain locations. On the other hand, electricity is a necessity throughout the natural gas supply chain, including at production, pipeline, processing, and distribution facilities. Reliability of supply, transportation constraints, and the integrity of existing infrastructure are some of the issues surrounding the electricity and natural gas interdependencies.

Both electricity and natural gas sector stakeholders in government and private sectors have undertaken a wide variety of approaches to address these concerns, including reliability assessments, interdependency studies, coordinating activities, as well as policy reforms to enhance the coordination and scheduling of natural gas pipeline capacity with electricity markets.[42] With the abundant production of natural gas, infrastructure expansions are underway to deliver natural gas to meet market demands. However, some supply constraints still remain due to certain siting, permitting and funding challenges.

4.2.3 Regional Coordination

In addition to the national unity of efforts in critical infrastructure security and resilience, regional coordination is important, especially in responding to actual events. Various regional initiatives are aimed to enhance regional coordination, address cross sector interdependencies, and facilitate incident response. One such effort is the DHS-led RRAP, which is a cooperative, interagency assessment of specific critical infrastructure that combines regional analysis of the surrounding infrastructure.[43] The RRAP evaluates critical infrastructure from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resilience characteristics, as well as regional capabilities and gaps. DHS staff lead the RRAP assessments in collaboration with SLTT organizations, SSAs, and infrastructure owners and operators. The information collected in the RRAP assessment is protected from public disclosure under the Protected Critical Infrastructure Information Act and cannot be used for regulatory purposes.

Similarly, the Pacific Northwest Economic Region (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 critical infrastructure regional protection projects.

---

[40] See Section 4.2.3 for more discussion on the RRAP.
[41] "Dams and Energy Sectors Interdependency Study," September 2011, U.S. DOE and DHS, http://energy.gov/sites/prod/files/Dams-Energy%20Interdependency%20Study.pdf (accessed Mary 12, 2015).
[42] Natural Gas and Electric Coordination, FERC, http://www.ferc.gov/industries/electric/indus-act/electric-coord.asp (accessed May 21, 2015).
[43] "Regional Resiliency Assessment Program (RRAP)," DHS, http://www.dhs.gov/regional-resiliency-assessment-program (accessed July 14, 2014).

In the Electricity Subsector, cooperation between utilities on a regional basis has been taking place for many years. Investor-owned utilities (IOUs) operate through the eight Regional Mutual Assistance Groups (RMAGs)—Great Lakes, Mid-Atlantic, Midwest, New York, Southeastern Electric Exchange, Texas, Western Region, and Wisconsin. Canadian utilities have also participated in the RMAGs. Municipal utilities engage their Mutual Aid Playbook to coordinate disaster response and recovery. Cooperative utilities coordinate mutual aid through State groups; the IOUs, municipals, and co-ops coordinate jointly on a national level through their respective trade associations.

Natural gas utilities participate in regional and national mutual assistance programs, which provide emergency support as needed in the event of service disruptions beyond the recovery capacity of the impacted gas utility. In a time of need, the impacted utility reaches out locally or regionally to get assistance. Should the need exceed the regional capacity, assistance is sought at the national level. In the aftermath of Hurricane Sandy in 2012, the industry led an unprecedented level of efforts to mobilize resources, in which DOE also played a key supporting role.[44]

Additionally, AGA holds an annual National Mutual Assistance Drill where the natural gas industry and regional associations participate in a disaster scenario simulation that tests the effectiveness of existing mutual assistance programs and further enhances the emergency response efforts of North America's natural gas utilities. In addition to these regional coordination efforts, the Energy Sector has a variety of ongoing activities to address international interdependencies and enhance international coordination as discussed in the following section.

4.2.4 International Interdependency and Coordination

Energy infrastructure interdependencies cross international borders in many ways. The United States depends on cross-border flows of energy resources to meet its total energy requirements. In addition, the energy system is supported by and critically dependent upon global flows of information, knowledge, and investment capital.[45] The United States relies on the import of critical technologies and equipment, such as LPTs, as well as many key raw materials that are essential to the manufacturing of certain electrical infrastructure. Further, many oil companies have facilities in various global locations that operate under different foreign sovereignties. Therefore, Energy Sector owners and operators stay cognizant of the international interdependency issues, including the key supply chains, as well as changing economic, political, and regulatory conditions, and continue to develop strategies to mitigate potential risk resulting from them.

Therefore, it is critical that the United States works closely with other countries to reduce physical and cyber vulnerabilities that could affect the U.S. energy infrastructure. In 2011, the Administration released the 2011 International Strategy for Cyberspace, which highlighted the need to develop a U.S. government position for an international cybersecurity policy framework and to strengthen international partnerships to create initiatives that would address cybersecurity activities.[46] DOE, in conjunction with DHS, Department of State, Department of Commerce, and other Federal agencies, cooperates in bilateral and multilateral forums with other countries. North America has an integrated system of oil and natural gas pipelines and electric transmission lines. Pipeline interconnections between the United States and Canada and between the United States and Mexico move considerable volumes of natural gas (and also oil in case of Canada) between the countries. This also requires coordination to ensure that protective measures across borders provide

[44] "Overview of Response to Hurricane Sandy-Nor'Easter and Recommendations for Improvement," DOE, February 26, 2013, http://energy.gov/sites/prod/files/2013/05/f0/DOE_Overview_Response-Sandy-Noreaster_Final.pdf (accessed January 15, 2015).
[45] Maull, Hanns, "Global Shift: The Challenges of Energy Interdependence and Climate Change," Transatlantic Academy Paper Series, September 2011, http://www.gmfus.org/wp-content/blogs.dir/1/files_mf/maull_climateenergy_aug11_final_web1.pdf (accessed June 30, 2014).
[46] "The International Strategy for Cyberspace," the White House, May 11, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed July 9, 2014).

adequate risk reduction across the full length of these systems. DHS Transportation Security Administration and DOE work together with NRCan and PS Canada to coordinate matters related to pipeline safety and security.

The integrated electric transmission system allows the United States and Canada to pool resources to improve electric reliability. The United States and Canada have a well-established history of collaboration and cooperation on electricity reliability. In 2008, the United States and Canada signed the Canada-United States CIP Framework for Cooperation to promote an integrated approach to critical infrastructure security and resilience through an enhanced coordination of activities and dialogue among cross-border stakeholders.[47] The framework includes energy, as well as transportation and other sectors' infrastructure, and is evidence of the mutual commitment by each country to work for the protection of shared critical infrastructure. In the Electricity Subsector, the NERC CIPC includes international members from Canada.

Similarly, the Trilateral Electric Reliability Oversight Group, established in 2004 stemming out of the U.S.-Canada Power System Outage Task Force, includes participation from the Canadian Federal-Provincial-Territorial Electricity Working Group, DOE, the Federal Energy Regulatory Commission (FERC), and the Government of Mexico. As a forum for identifying and resolving reliability issues in an international, government-to-government context, this group develops principles to guide the establishment of a reliability organization that can function on an international basis, coordinates on the electric reliability standards process, and consults on policy and regulatory issues surrounding reliability.

In addition, DOE and NERC have also participated in a series of the Electric Infrastructure Security Summit in the United States and in the United Kingdom to assess resilience for wide-area grid outages from electromagnetic threats and other hazards.[48] Also, another international forum called the International Electricity Infrastructure Assurance Forum shares lessons learned and best practices regarding a wide variety of critical infrastructure threats and vulnerabilities. The group includes experts from Australia, Canada, New Zealand, the United Kingdom, and the United States.

4.3 Information Sharing and Communication

Ensuring timely, reliable, and secure information exchange has been one of the top priorities of the Energy Sector. Both the industry and the government need credible, timely, and actionable threat and risk information to ensure that the most appropriate security investments, programs, and decisions are made to secure sector assets. Information on vulnerabilities, threats, and consequences is, by nature, sensitive. Unless both public and private sector partners trust that shared information will be strictly protected and used only for agreed-upon purposes, the costs of sharing sensitive information could be seen to outweigh the benefits, and the partnership could fail.

Goal:

"Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making."

Trusted relationships among decision makers who implement risk management programs provide the most effective foundation for coordinated response functions and effective information sharing programs. During times of increased security posture or emergency situations, the trusted relationships between government and industry are extremely valuable. 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.

Many information sharing mechanisms exist between government and industry, within the critical infrastructure community, as well as through various industry trade associations. The Homeland Security Information Network (HSIN)

[47] "Canada-United States CIP Framework for Cooperation," DHS and Public Safety Canada, September 2008, https://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf (accessed September 25, 2014).
[48] Electric Infrastructure Security Summit, http://www.eissummit.com/ (accessed September 18, 2014).

provides a national platform to share homeland security information with sector partners. HSIN is a secure, Web-based platform for Sensitive-But-Unclassified information sharing and communication among Federal, SLTT, and private entities, as well as international partners. HSIN is just one of many information sharing mechanisms for critical infrastructure.

There are three key private sector information sharing tools in the Energy Sector—the Electricity ISAC (E-ISAC), ONG ISAC, and Downstream Natural Gas ISAC (DNG- ISAC). These three ISACs serve the same objectives—collaboration, trusted information sharing community, and timely threat intelligence analysis. Industry participation in the ISACs is voluntary. Industry is cautious in sharing sensitive information and providing specifics regarding ongoing and planned protective programs; however, the E-ISAC, for example, has established precautionary measures to prevent security information shared with the E-ISAC from being used for CIP compliance purposes. Specifically for cybersecurity, DOE and the ESCC have developed the Cybersecurity Risk Information Sharing Program to facilitate the timely sharing of cyber threat information and the development of situational awareness tools to enhance the Electricity Subsector's ability to identify, prioritize, and coordinate the protection of its critical infrastructure.

As the SSA, DOE acknowledges the value of these trusted relationships and continues to work closely with industry, States, DHS, FERC, and other agencies to develop suitable information exchange policies, regulations, and procedures. The goal is to protect all industry information against inappropriate disclosure. In addition to the three ISACs, information sharing and communication occur through various means in the Energy Sector.

4.4 Critical Infrastructure Resilience and Preparedness

Incident response planning and exercise is an essential part of the Energy Sector's resilience because preparation minimizes the disruption of critical infrastructure functions and associated consequences during an incident. Many incident response initiatives are in place to help maintain a robust, secure, and reliable energy infrastructure that is also resilient—i.e., able to restore services rapidly in the event of any disaster. The core of such preparedness and planning exercises is flexibility and adaptability to incorporate new information such as a changing risk environment, lessons-learned, and best/effective practices. These programs are held at the Federal, regional, SLTT, and private levels, and are designed to prepare for and respond to incidents in order to minimize impacts resulting from a disaster. DOE and other government partners work with their industry partners for planning and encourage them to participate in the exercises.

In the Federal Government, ESFs provide the structure for coordinating Federal interagency support for a Federal response to an incident. They are mechanisms for grouping functions most frequently used to provide Federal support to States and Federal-to-Federal support, both for declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents.[49] DOE is the lead agency directing ESF-12 (Energy),[50] which assists the restoration of energy systems and provides an initial point-of-contact for the activation and deployment of DOE resources. Through ESF-12, DOE helps transitioning from steady state to incident response and recovery. These activities are performed pursuant to the Stafford Act, Homeland Security Presidential Directive—5 Management of Domestic Incidents and the NRF. Further, as part of its efforts to enhance situational awareness of potential disruptions of critical energy infrastructure and resources, DOE developed the Environment for Analysis of Geo-Located Energy Information (EAGLE-I), an energy infrastructure monitoring capability.[51]

Goals:

"Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services."

"Promote learning and adaptation during and after exercises and incidents."

In addition to government programs, individual asset owners and operators have their own company- and facility-level response plans that are specific to their assets. As part of their everyday operation, owners and operators develop and apply facility and system risk assessment methodologies, and they prioritize their assets for protection and plan for possible restoration and recovery from anticipated threats. In addition, the industry, as appropriate, uses insurance mechanisms to help mitigate the cost of impacts to their assets and to support restoration and recovery.

To test these plans and response frameworks, government and industry participate in different exercises that may be organization-specific, regionally-focused, sector-specific, national, or international in nature. Exercises, such as DHS' Cyber Storm exercise series and NERC's Grid Security Exercise series, allow stakeholders to consider scenarios that impact their operations and require them to test response, mitigation, and recovery activities.

Energy Sector partners, including private owners and operators, consider many types of hazards in their resilience/recovery plans, including natural hazards, which are likely to occur with little or no warning. For that reason, industry activities focus on improved resilience through design, inventory, equipment sharing, and operational actions, as well as restoration and recovery preparation. In addition, redundancy is built into both electricity and oil and natural gas systems to enhance the resilience of operation and the reliability of service.

[49] "Emergency Support Function Annexes: Introduction," FEMA, http://www.fema.gov/media-library-data/20130726-1825-25045-0604/emergency_support_function_annexes_introduction_2008_.pdf (accessed September 10, 2014).
[50] "Emergency Support Function #12 – Energy Annex," FEMA, https://www.fema.gov/pdf/emergency/nrf/nrf-esf-12.pdf (accessed September 10, 2014).
[51] EAGLE-I is a web tool that automatically gathers real-time electrical grid service status data from company websites and organizes it into an easy to read picture of electrical service status nationwide. Covering 75 percent of all U.S. electricity customers, it provides real-time information about the grid, helping to effectuate incident response and recovery.

5 RESEARCH AND DEVELOPMENT PRIORITIES

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 securely deliver energy are among the most technologically sophisticated of any sector and have long been faced with the challenge of providing high levels of productivity and reliability against weather and other physical threats. While increased use of automation, IT, telecommunications, and other electronically-enabled devices are helping these systems to become more efficient and resilient, they also create vulnerability to malicious and unintentional cyber threats.

Federal R&D investments are available across government agencies and are, for the most part, coordinated with relevant investment 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 help identify priorities in cooperation with sector partners. In particular, Federal R&D seeks to fill gaps and stimulate private investment.

Maintaining and improving the resilience and security of the critical energy infrastructure is a shared responsibility among government entities and energy owners and operators.[52] In addressing these challenges, energy owners and operators work closely with governments, national laboratories, universities, industry organizations, and other key stakeholders to drive technological innovation throughout the sector.

5.1 R&D for Resilience

One of the key goals of R&D in the Energy Sector is to increase all-hazards, infrastructure resilience. Specifically to natural disasters, the objective is to reduce the social consequences as expressed in terms of impact to quality of life, economic activity, and national security, beyond the impact to the energy system performance itself. As the Nation's energy infrastructure is mostly owned and operated by the private sector, and because the Nation's economy and security depend on reliable supply of energy, R&D for energy infrastructure resilience is a shared responsibility. Thus partnerships across all levels of government and the private sector are required for the life cycle of R&D, from planning and development to implementation.

The Energy Sector has held collaborative activities across government agencies and the private sector in assessing resilience and evaluating the R&D needs and opportunities. The NIPP 2013 clearly lays out a Call to Action consisting of 12 activities identified collaboratively by government and the private sector. The Call to Action is intended to guide efforts to achieve national goals to enhance national critical infrastructure security and resilience. These activities build upon partnership efforts, innovate in managing risk, and focus on outcomes. Call to Action #10 hones in on R&D and directs the Federal Government to take into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. Areas of interest include improving the security of cyber technology, enhancing modeling capabilities of incident and threat scenarios (including cascading effects cross sectors), incentivizing cybersecurity investments, and designing features that strengthen all-hazards security and resilience. Understanding and addressing interdependencies is important for the Energy Sector because it serves as a

[52] The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," PPD-21, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed December 1, 2014).

lifeline function for other sectors. Just as critical is understanding upon which other critical infrastructure sectors the Energy Sector is dependent to ensure proper coordination and resiliency planning. R&D needs for Energy Sector resilience exist in the following areas:

- Enhance System Design for Resiliency. Innovative R&D is needed for cost-effective hardening measures (e.g., new materials and higher design and construction standards), as well as for resilient design tools to enable energy infrastructure designers to prioritize cost-effective system upgrades and expansions to minimize social consequences.
- Improve Preparedness and Mitigation Measures. This includes new tools for resilience assessment, monitoring of predictive failure modes of energy equipment and systems (such as synchrophasors and frequency disturbance recorders for monitoring conditions of power delivery networks), and damage prediction models. Improved flexibility and robustness measures such as power electronic-based controllers, energy storage, and microgrids have also been identified.
- Improve System Response and Recovery. Improved situational awareness and its prerequisite of a resilient communications infrastructure are two key areas needed for strengthening Energy Sector resilience over the next ten years.[53] Other R&D areas include new energy management systems and optimization tools for restoration prioritization.
- Analyze and Manage Interdependencies. A comprehensive framework for interdependency modeling and simulation can support the integration of multiple disparate models and simulations to conduct cross infrastructure analysis to address the threat assessment, preparedness, mitigation, response, and recovery issues. This type of framework can build on models and simulation tools already available to address aspects of individual infrastructure.

5.2 R&D for Physical Security

The NIPP 2013 recognizes that our Nation's critical infrastructure is largely owned and operated by the private sector. Collaboration is vital due to the urgency of the potential threats to the Energy Sector, including multiple, coordinated physical attacks and electromagnetic pulse (EMP) events. Physical threats emphasize the need for innovative tools and technologies that harden critical infrastructure against high-impact risks. DOE works with DHS Science and Technology Directorate (S&T), other Federal agencies, energy asset owners and operators, trade organizations, vendors, National Laboratories, universities, and research organizations to develop the capabilities necessary to secure the homeland against terrorism, other manmade disasters, and physical threats.

Due to other critical infrastructure sectors' high reliance on energy, there will always be concerns about high-impact, low-frequency events and their respective effects. Specifically, in regards to electricity and the bulk power system, opportunities should be tapped that expand on existing work in monitoring and analysis of geomagnetically-induced currents, the impact of GMD, EMP, and other physical threats on critical grid components including LPTs and bushings.

[53] The Energy R&D Workshop, Enhancing Resilience to Natural Disasters, was jointly sponsored and held by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the DOE Office of Electricity Delivery and Energy Reliability (OE) in July 2013 with over 40 stakeholders representing the electric, oil, and natural gas industries, as well as State and Federal Governments. Key takeaways from the workshop are documented in the workshop report, available at http://energy.gov/sites/prod/files/2014/07/f17/2014ResilientGridWorkshop-FinalReport.pdf (accessed November, 26, 2014).

DOE and sector stakeholders will continue to work collaboratively to identify and address future challenges of the Energy Sector as the threat environment continues to evolve. Leveraging the long history of collaboration among Energy Sector stakeholders will enable the sector to better anticipate and meet future challenges.

5.3 R&D for Energy Delivery Systems Cybersecurity

Cybersecurity R&D for energy delivery systems requires collaboration among diverse Energy Sector stakeholders—including utilities, suppliers, national laboratories, universities, and government—that work at the intersection of power systems engineering and the computer science of cybersecurity.

Energy Sector stakeholders from public and private sector collaboratively developed the *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*.[54] The Roadmap articulates the sector's vision that "by 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions." It also presents a set of milestones that guide Energy Sector cybersecurity activities in five strategic areas: building a culture of security, assessing and monitoring cybersecurity risks, developing and implementing new protective measures to reduce risks, managing incidents, and sustaining security improvements. Given the evolving cyber vulnerability and threat landscape, this Roadmap may need to be revised to ensure that the Energy Sector remains on track.

Energy Sector stakeholders use a Roadmap approach to identify needs and to encourage the research, development and demonstration of next-generation cybersecurity capabilities to address evolving cyber threats, the introduction of new power system technologies, and the use of legacy devices in ways not previously envisioned. DOE partners with energy infrastructure owners, operators, suppliers, national laboratories, and universities to improve cybersecurity capabilities that work well within energy delivery systems. Examples of research that are being used today in the Energy Sector include technologies that detect intrusion for smart meter communications and help prevent unexpected cyber activity. DOE plans to engage Energy Sector stakeholders, perform research at the intersection of power systems engineering and the computer science of cybersecurity, and maintain alignment with the Energy Sector's Roadmap.

[54] Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," DOE, September 2011, www.controlsystemsroadmap.net (accessed December 18, 2014).

6 MEASURING PROGRESS

Measuring progress in advancing security and resilience goals has been one of the core guiding principles of the national risk management framework for critical infrastructure. The Energy Sector continues to improve approaches to measure progress toward achieving the critical infrastructure security and resilience goals. An effective performance measurement system identifies appropriate metrics for measuring progress, collects relevant data, and uses that information to improve performance and provide accountability. DOE and its sector partners continue the process of identifying relevant information and possible metrics that are specific to the sector. This section provides a brief highlight of the current and planned security and resilience activities in the sector, how they contribute to achieving national and sector goals and priorities, and some of the ways in which each subsector tries to measure its progress toward critical infrastructure security and resilience goals.

6.1 Sector Activities

In the Energy Sector, policies and programs are developed through a collaborative effort based on the sector's risk management, security, and resilience goals. The Energy Sector has numerous activities that support the sector's risk management goals and priorities. In 2014, Energy Sector identified approximately 170 ongoing programs. Table 6-1 provides a sample of such activities, and how they support the joint national priorities. All of these programs and activities support one or more of the national critical infrastructure security and resilience goals and priorities. See appendix A for the mapping of the joint national priorities and the energy sector priorities. Due to the large number of programs and the sensitive nature of certain information, the comprehensive list of programs is not included in this document; however, additional information and points of contacts on specific programs may be made available to appropriate Energy industry and government partners with a need.

Table 6-1 Energy Sector Activities Mapped to Joint National Priorities

Joint National Priority	Energy Sector Activity
A, B, C, D, E	There are some 170+ ongoing activities underway by energy sector partners in support of joint national priorities in the NIPP 2013. With more than 85 percent of energy sector assets owned and operated by the private sector, owners and operators play a key role in cooperation with government and SLTTGCC partners in their effort to improve the sector's reliability and resiliency against the evolving challenges—natural and manmade—the sector is facing.
A, E	DOE, working with sector partners, was the first agency to release the NIST Framework Implementation Guidance. DOE has developed a voluntary cyber tool to help asset owners and operators assess their strengths and weaknesses.
A, B, C, E	Both electricity and oil and natural gas subsectors have supported the ISACs to share threat information and developed playbooks to help coordinate industry and government responses to energy emergencies.
A, D	NERC developed (and FERC approved) mandatory physical protection and cybersecurity Reliability Standards for the electricity industry.
A, E	The DHS Enhanced Critical Infrastructure Protection program continues its visits to energy sites with a tool to identify possible physical and cyber weaknesses, and provides recommendations to site operators.
B, C, E	DOE and the ONG SCC are working to implement the recommendations resulting from the National Petroleum Council report, "Enhancing Emergency Preparedness for Natural Disasters." The recommendations identify mechanisms for the U.S. government and industry to improve communication and coordination in responding to energy system disruptions.

D	Metrics tracking for the electricity subsector is well established by the NERC with yearly updates and ongoing efforts to improve comparability and quality of reporting. The ONG SCC is using Survey Monkey to assess efforts in the oil and natural gas sectors. Trade organizations in both electricity and oil and natural gas industry have or are developing approaches to track and encourage progress of their members.
A, B	Energy Sector trade organizations are very active on an ongoing basis with their members addressing both cyber and physical security issues. Exercises as well as targeted training opportunities are a regular activity.
B, C, E	Lessons learned from previous emergencies are used to help educate asset owners and operators. Increasing dialogue with other sectors and agencies has become a focus of efforts including the need to include SLTT representatives and Canada. Supply chain issues are being addressed led by the ESCC and the ONG SCC to identify issues, interdependencies, and barriers to improving restoration and recovery from energy emergencies.
A	The Energy Sector remains vigilant to the possibility of low frequency but high impact events including GMD/EMP, earthquakes, pandemics and combined physical and cyber threats.
B	The DOE Emergency Response Organization working with FEMA supports ESF #12 activations on an ongoing basis. Over 70 DOE personnel have been trained to provide expertise during events to speed restoration and recovery. Past activations have included hurricanes, tornadoes, wildfires, and tropical storms.
B, D, E	DOE's EAGLE-I is one of the most widely used real-time emergency response tools in the Federal government with more than 800 users. EAGLE-I has two components—a dashboard to provide real time information to users to allow monitoring of the energy infrastructure and a mapper to display assets and components of the energy infrastructure along with real time hazards.

The effectiveness of these critical infrastructure risk management activities are measured at various levels, ranging from broad, national perspectives to organization-specific assessments. The Energy Sector stakeholders continue to evaluate the performance of various activities as well as their priorities to ensure that their efforts are helping the sector to advance towards a more resilient infrastructure. Acknowledging the difficulties in collecting meaningful quantitative data for such evaluation, DOE collaborates with the industry stakeholders and utilizes existing data to evaluate the performance and reliability of its infrastructure.

6.2 Measuring Progress and Effectiveness

The Energy Sector consists of a diverse group of assets and systems that are owned and operated by many organizations and overseen under various jurisdictions. The complex operating structure, in addition to the evolving threat and risk environment, make it difficult to accurately assess and measure the security and reliability posture of the sector and subsectors. Energy Sector partners have made considerable efforts and progress in the development of performance metrics, which will allow DHS, DOE, and sector partners to assess the sector's progress toward meeting its critical infrastructure security and resilience goals and objectives.

6.2.1 Electricity Subsector

The Electricity Subsector, through DOE and NERC, has extensive historical data—both quantitative and qualitative—which is used to assess the availability, reliability, resilience, and integrity of essential services. Using a wide variety of indicators, the NERC data can identify actual and potential threats and risks to the Electricity Subsector. According to the historical data, weather-related events, including lightning and tropical storms, have historically been the biggest threat to the reliability of the grid and the critical infrastructure. Between 2008 and 2013, transmission outages caused by weather-related events and misoperation of the protection system were the largest known contributors to transmission outages.[55]

[55] "State of Reliability 2014," NERC, May 2014, http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2014_SOR_Final.pdf (accessed April 14, 2015).

Although cybersecurity threats have yet to cause a significant damage to the reliability of the electric system, NERC and the Electricity Subsector have placed a heavy emphasis on addressing cybersecurity issues. This could be an indication that while scarce, cybersecurity incidents have the potential to significantly impact the reliability of the grid and the financial health of the company that is targeted.

The identification of these threats could help support making risk-informed decisions, enabling prioritization of issues, and aligning resources to address them. Further, these metrics can be useful in developing and implementing appropriate steps to help reduce and manage risks to reliability as well as enhance the security of critical infrastructure. While the Electricity Subsector has devoted considerable resources and efforts in the areas of risk assessment and infrastructure security, its development of security metrics remain a work in progress.[56]

6.2.2 Oil and Natural Gas Subsector

In the ONG Subsector, the ONG SCC has partnered with DOE, the Energy SSA, in the development of security metrics to assess the security and preparedness of the ONG Subsector. The metrics will not only assist DHS in developing an assessment of the security and resilience posture of the Nation's critical infrastructure as stipulated in the NIPP, such metrics can also provide value to the Energy Sector as a whole by highlighting the steps sector partners have taken to improve security and resilience and also by identifying potential gaps. Capturing metrics that provide a picture of the ONG Subsector as a whole is challenging, as the industry is vastly diverse and consists of a large spectrum of business models, company sizes, applicable regulations, and operations.

Many sites/facilities within the ONG Subsector are subject to one or more of the following regulations: CFATS; MTSA; Transportation Security Administration's Freight Rail Security Rule; Transportation Worker Identification Credential; and DOT's Hazardous Materials Security Planning/Training HM-232. In addition to these regulatory measures, many of the ONG owners and operators participate in a wide variety of voluntary security initiatives offered through national, State, regional, local, and industry organizations.

Taking these mandatory and voluntary efforts into consideration, in 2010, the ONG SCC developed high-level cyber and physical security metrics applicable to activities that span the subsector. The survey respondents mirrored the diversity of the ONG Subsector, taking into consideration size of operation, applicable regulations, participation in voluntary security methods, and identification of policies in place for assessment of vulnerabilities and security threats. Additionally, the metrics addressed the level of engagement of first responders in Emergency Response Plans, as well as ongoing engagement in exercises and training/lessons learned. The goal of the effort was to develop outcome-based metrics that focus on objectives established by the ONG Subsector, which include identifying and prioritizing subsector opportunities, needs, and practices that advance the subsector's security posture. The ONG Subsector metrics survey is scheduled to be conducted again in 2015.

[56] For more information on NERC reliability indicators, see http://www.nerc.com/pa/RAPA/ri/Pages/default.aspx (accessed May 29, 2014).

APPENDIX A:
CONTRIBUTION OF SECTOR PRIORITIES TO JOINT NATIONAL PRIORITIES

Electricity Subsector Priorities	Oil and Natural Gas Subsector Priorities	Joint National Priorities				
		A Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	B Build Capabilities and Coordination for Enhanced Incident Response and Recovery	C Strengthen Collaboration across Sectors, Jurisdictions, and Disciplines	D Enhance Effectiveness in Resilience Decision Making	E Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities
Tools and Technology	Partnership Coordination	√	√ √	√	√	√
Information Flow	Implementation and Communication	√	√ √	√		√ √
Incident Response	Identification of Sector Needs, Gaps, and/or Best Practices		√	√	√	√
	Information Sharing	√	√	√		√
	Business Continuity	√	√		√	