Annex 8:

2008 Sector CIKR Protection Annual Report

for the Energy Sector

July 1, 2008

Homeland Security

Department of Energy

This page intentionally blank

Contents

Foreword

Our Nation's economy and its population's well-being depend heavily on the products and services supplied by the Energy Sector. Every citizen expects reliable and affordable energy, and a disruption to the energy supply, whether from man-made or natural causes, can have a profound impact on the population's quality of life, conduct of business, and even the Nation's security.

The U.S. Department of Energy (DOE) leads the Federal Government's efforts to advance the energy security of the United States. This task is done in partnership with Energy Sector security partners in Federal, State, local, tribal, and Territorial governments and, most importantly, in close cooperation with private sector asset owners and operators, who represent more than 85 percent of the Nation's Energy Sector assets.

This *2008 Sector CIKR Protection Annual Report for the Energy Sector* provides a rich overview of the many efforts underway to ensure a secure, reliable, and resilient energy infrastructure. Key energy systems are best protected through effective public and private partnerships. These partnerships lead to the activities necessary to improve energy system reliability, survivability, and resiliency. In addition, the restoration and recovery of energy services have been a key focus of ongoing efforts by Energy Sector partners.

This annual report was completed in close cooperation with Energy Sector security partners and members of the Energy Sector Government Coordinating Council (GCC), Oil and Natural Gas Sector Coordinating Council (SCC), and Electricity SCC. The Energy Sector security partners provided material for this report and had the opportunity to review its contents in the draft stage. Their cooperation and partnership have become the hallmark of Energy Sector activities conducted to implement the Energy Sector-Specific Plan (SSP). These activities are described in the following sections.

This page intentionally blank

Executive Summary

The U.S. Department of Homeland Security (DHS)[1] completed the National Infrastructure Protection Plan (NIPP) in June 2006, in accordance with Homeland Security Presidential Directive 7 (HSPD-7). The NIPP sets forth a comprehensive risk management framework and defines critical infrastructure protection roles and responsibilities for DHS; Sector-Specific Agencies (SSAs); and other Federal, State, local, tribal, Territorial, and private sector security partners. In accordance with the NIPP, the DOE — designated as the Energy SSA — led the efforts in developing the Energy SSP and this *2008 Sector CIKR Protection Annual Report for the Energy Sector.* This 2008 annual report, developed as part of the NIPP framework, serves as an update to the Energy SSP and reflects the continual significant progress accomplished since the last annual report was submitted in July 2007.

DOE, in its role as the Energy SSA, has built a relationship of trust with government and industry security partners throughout the working process under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC). The Electricity SCC, Oil and Natural Gas SCC, and Energy GCC played vital roles in completing both this annual report and the Energy SSP documents. The Electricity SCC represents more than 95 percent of the electric power industry, and the Oil and Natural Gas SCC represents more than 98 percent of that industry. The GCC, chaired by DOE, represents all levels of government including State, local, tribal, and Territorial sector security partners.

The Energy Sector has established a unified vision and six sector security goals as a framework for developing and implementing effective preparedness, protective, and recovery measures. Because the Energy Sector consists of thousands of different types of assets that are geographically dispersed and connected by systems and networks, an understanding of interdependencies within the Energy Sector and across the Nation's other critical infrastructure sectors is critical for energy security planning.

The Energy Sector already has more than 110 programs sponsored by dozens of public and private organizations that support Sector security, reliability, survivability, and resiliency goals. The programs fall within four main categories: information sharing and communication, physical and cyber security, coordination and planning, and public confidence. The Energy Sector will continue to implement effective protective measures as it assesses the Sector's security needs, develops programs, and finds long-term solutions, including research and development (R&D). Moreover, because improved infrastructure security and resilience have become increasingly significant objectives of the Energy Sector's technology R&D, the Federal R&D investments will continue to be coordinated with those of the private sector in order to leverage available resources and create an effective national R&D strategy for critical infrastructure protection.

Perhaps the most valuable aspect of the SSP development process has been the establishment of open communication and the growing trusted relationship between government and industry. DOE's Office of Electricity Delivery and Energy Reliability (OE) has taken the responsibility of

[1] A list of acronyms used in this report can be found in attachment A; Energy Sector protective programs and activities are described in attachment G; references and resources are listed in attachment J.

the Energy SSA and oversees all activities associated with the NIPP and the Energy SSP. In doing so, DOE-OE maintains a close partnership with the Electricity SCC, Oil and Natural Gas SCC, and governmental partners through the CIPAC. This partnership will continue to facilitate a unified national effort to implement the Energy Sector's protective programs for critical infrastructure and key resources (CIKR) and accomplish its security goals.

Section 1: Sector Security Goals and Priorities

1.1 Sector Security Vision and Goals

The Energy Sector, together with the Energy Government Coordinating Council (GCC), Electricity Sector Coordinating Council (SCC), and Oil and Natural Gas SCC, established a unified vision and a set of six security goals as the cornerstone for developing the Energy Sector-Specific Plan (SSP). Prepared by the U.S. Department of Energy (DOE) with government and industry partners, the Energy SSP is a critical component of the Department of Homeland Security's (DHS's) National Infrastructure Protection Plan (NIPP). The vision and goals identified in the Energy SSP have provided a framework for the continual development of effective protective measures for enhancing the security and preparedness of our Nation's energy infrastructure (table 1-1).

Table 1-1: Energy Sector Security Vision and Goals

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

1.2 Sector CIKR Risk Profile[2]

DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces a risk profile for each critical infrastructure and key resources (CIKR) sector to inform each sector's security priorities. Working closely with the U.S. Intelligence Community as well as the SSAs, HITRAC integrates and analyzes information on threats to assess potential vulnerabilities to and consequences from a terrorist attack on each sector.

HITRAC's risk profile, however, considers only the threat from a terrorist attack. The Energy Sector's electricity, oil, and natural gas assets are also vulnerable to natural hazards, such as hurricanes, earthquakes, fires, tornadoes, ice storms, and other events related to extreme weather conditions.

1.2.1 Oil and Natural Gas Subsector

Hurricanes are the most frequently disruptive natural hazards for the Oil and Natural Gas Subsector, often causing the preemptive shutdown of facilities in an area, even if the facilities themselves are not directly affected by the storm. This Subsector has significantly reduced its vulnerability to adverse events and increased the overall resiliency of its product supply chain by building in redundancy of operations, general geographical dispersion of assets, and the ability to adjust to and compensate for lost assets. As a result, damage to one or several refineries, offshore platforms, or other assets would not be likely to extensively affect the gasoline supply chain.[3]

2007 Oil and Natural Gas Statistics

Crude oil imports: 66 percent

Number of refineries: 149

Number of refineries with capacities of more than 100,000 barrels of oil per day: More than 60

Product pipelines: 116,000 miles

Natural gas imports: 16 percent

Number of gas processing plants: More than 550

Gas distribution pipelines: 1,175,000 miles

The Oil and Natural Gas Subsector demonstrated its resiliency by the speed with which the Gulf Coast energy infrastructure recovered from Hurricanes Katrina and Rita in 2005, despite widespread damage and destruction affecting extraction, production, and transportation assets along the Gulf Coast and in the Gulf of Mexico.

2 Attachment B provides an updated overview of the Energy Sector.

3 This threat assessment focuses on national impacts. Regional or state impacts from specific refinery outages could be much more significant.

1.2.2 Electricity Subsector

In addition to terrorist attacks, the Electricity Subsector is especially prone to natural hazards and cyber attacks. Hurricanes, tornadoes, fires, floods, and even localized thunderstorms can cause significant outages in the power grid. However, the power system is designed to protect itself by detecting abnormal conditions and shutting down localized sections or components before significant damage is incurred.

2006 Electricity Statistics

Number of power plants: More than 5,300

Installed generation capacity: 1,075 gigawatts

Transmission lines: More than 211,000 miles

Source: DOE Energy Information Administration (EIA).

Electric power assets are potentially vulnerable to cyber attacks because the electricity infrastructure is highly automated and controlled by utilities and regional grid operators who rely on sophisticated energy management systems. For example, the Electricity Subsector's control system networks are connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the networks' vulnerability to direct cyber attacks that could potentially disrupt power. Insider cyber threats, such as those initiated by current or former employees, also pose a unique security risk to the Electricity Subsector. Efforts are well underway to implement measures to reduce such risks. These include incorporating protective programs, such as passwords, virus protection, and intrusion detection systems. Mandatory standards promulgated by the North American Electric Reliability Corporation (NERC) are also being implemented.

A large-scale interruption to the national electric power supply is unlikely because of the excess capacity and redundancy built into the electric power system. Electric power assets are dispersed throughout North America as a system, thus allowing the electrical power grids to maintain operations nationally. Therefore, even if individual assets may be vulnerable, the Subsector's critical systems are generally resilient and would be able to withstand damage from terrorist attacks or natural hazards. Also, planning for speedy restoration of power has been an important area of focus in industry efforts, which adds to the resilience of the Subsector.

Although the resilience and system-based nature of the Electricity Subsector would regionalize the consequences of any single attack against a power plant, an attack on multiple assets or critical systems within the Subsector could cause cascading consequences in other sectors. For example, the extent to which other sectors depend on electric power was evident in the widespread impact of the power outage on August 14, 2003, that struck the upper Midwest, eastern Canada, New York, and New England. The outage affected more than 50 million customers and lasted for up to five days in some areas.

1.3 CIKR Protection Gaps

HITRAC's Energy Sector risk profile provides a basis for examining possible protection gaps and challenges. In addition to those discussed in this section, the Energy SSP has identified a number of these gaps and challenges.

1.3.1 Issues of Concern

Efforts over the last year have highlighted a few issues that affect preparedness planning, and the way in which the activities to reduce the risks to and vulnerabilities of critical energy infrastructures are discussed. These issues also drive Energy Sector research and development (R&D) priorities, as well as nearer-term practical activities and measures, which include those discussed in the following sections.

1.3.1.1 Planning for All Hazards, Including Deliberate Attacks

The first concern is that cyber threats have been growing and continuously changing as the Energy Sector has become more reliant on automated systems, standard protocols, and off-the-shelf hardware and software. The nature of the future threats to and vulnerabilities of the Energy Sector is not known, and continuing attention and support for research in this area are necessary.

The second concern is that, although the NIPP clearly states that the planning approach should be an "all-hazards" approach, DHS direction and guidance reflect more of a "terrorism-centric" approach. Funding to State and local governments is targeted toward strengthening improvised explosive device (IED) attack deterrence, prevention, and protection capabilities and improving preparedness planning. Under one grant program, proposals must require the implementation of activities that support terrorism preparedness (by building or enhancing capabilities that relate to the prevention of, protection from, or response to terrorism) in order to be considered eligible. However, many capabilities that support terrorism preparedness simultaneously support preparedness for other hazards, and grantees must demonstrate this dual-use quality for any activities to be implemented under this program and not explicitly focus on terrorism preparedness.

1.3.1.2 Enhancing the Resiliency of the Energy Infrastructure

In the Energy Sector, the States, in particular, have been focused on the importance of building resiliency. This focus addresses both the ability of systems to rapidly recover and return to normal operations and the longer-term investments that allow this recovery to occur or that might mitigate the risk level. The development of recovery transformers for the Electricity Subsector is identified as a high R&D priority. From an Energy Sector perspective, resiliency should be a high priority and an integral element of planning and preparedness efforts. This theme was the focus of the April 2008 Workshop on Building Resiliency into Energy Assurance Planning.

1.3.1.3 Sustaining and Growing the Capability of State, Local, Tribal, Territorial, and Private Sector Preparedness

As a result of the planning and training efforts conducted over the last year, it is increasingly apparent that as State and local personnel leave and are replaced and as experience is gained and then lost, some effort is required to maintain a baseline level of capability. This effort in some way needs to be institutionalized at the State and local levels. One example of how this need is being addressed is the development of State energy assurance guidelines and similar guidelines for local governments. More such measures are needed, however, and this topic will be an issue for further discussion and evaluation with regard to its role in moving forward. The development of wide-area situational awareness, involving the visualization of actual or possible energy-related events, can be a considerable boon to Federal, State, local, and private sector security partners. The analysis of the potential impacts and interdependencies related to an event can also provide important information. The criticality of electricity to all CIKR sectors is well recognized, and developing ways of communicating information is a key factor in all preparedness and response activities.

1.3.1.4 Improving Regional Coordination

As indicated by all the work done over the last four years and as demonstrated by the regional energy emergency exercises that have been held, there is now a greater need for multistate coordination. Decision-support tools can help decisionmakers respond to energy-related events. Energy systems are, by their nature, multistate, and if they are damaged or destroyed, the effect tends to be regional. Greater attention to regional coordination, planning, and preparedness among energy security partners is needed. DHS has begun to recognize this need by providing some grant funds for multistate investments.

1.3.2 Electricity Subsector

The Electricity Subsector has been working to address possible damage to the utility infrastructure caused by both natural and man-made events. In this Subsector, natural events primarily affect the distribution system, but they may also occasionally affect transmission lines and towers. Industry standards for tower design and improved siting practices have helped decrease the number of incidences of damage to transmission lines and towers from natural events. Industry planning standards, which require redundancy and resiliency, have also helped reduce the likelihood of technical failures.

Increased manufacturing lead times for large power transformers have led the Electricity Subsector to focus its attention on ensuring that the industry has an adequate inventory of spares. The Subsector has developed a program called the Spare Transformer Equipment Program (STEP), through which participants are contractually obligated to maintain an adequate inventory of spare transformers and commit to sharing transformers with other utilities in the event of a terrorist attack. Under the terms of the contract, participants may voluntarily share transformers with other utilities for other reasons as well. STEP participants conducted an exercise in late

summer 2007 to identify the possible next steps to improve the industry's ability to recover from devastating disruptions. This program already represents over 70 percent of all large transformers in the United States. In addition, NERC has developed a voluntary database of transformers that can facilitate sharing of spares, alleviating the vulnerability of transformers.

1.3.3 Oil and Natural Gas Subsector

The Oil and Natural Gas Subsector has also faced a major challenge in addressing the need for backup generation and restoration capabilities in the event of natural disasters, terrorist attacks, or other causes. Companies are taking steps to ensure that backup power is more available and quickly transferable when needed, and they are exploring the option of equipment sharing on a regional basis in the event of a national emergency.

The Oil and Natural Gas Subsector faces the additional challenge of securing its maritime facilities; the United States, on an average, imports more than 60 percent of its petroleum and more than 13 percent of its refined petroleum products to meet its needs. The capacities of ports and harbors, as well as rail lines and inland waterways, are crucial to the security of energy systems.

1.3.4 Human Resources

Industry contingency planning and preparation for a possible influenza pandemic highlight the existing challenges in meeting staffing requirements and maintaining industry expertise. As the baby boomers start to retire, a significant number of industry experts could be unavailable, and strategies need to be developed to replace them. The Energy Sector has recognized the potential shortages of trained personnel. To address this challenge, several trade associations recently formed the Center for Energy Workforce Development, which is working with educational and other institutions to broaden the base of trained workers for energy jobs. The electric power industry has dealt proactively with shortages of skilled restoration crews by developing extensive mutual aid networks. The recovery from Hurricanes Katrina and Rita involved significant support and sharing of crews from the natural gas industry.[4]

1.3.5 Cyber Security

Security concerns relating to supervisory control and data acquisition (SCADA) systems and other protected energy systems have increased as systems that were originally built as standalone systems have become increasingly connected to corporate and other networks. To address this issue, the Energy Sector is working through the SCCs under the Critical Infrastructure Partnership Advisory Council (CIPAC) to implement DOE's *Roadmap to Secure Control*

[4] Attachment C provides information on pandemic planning. Attachment F describes security training opportunities.

Systems in the Energy Sector (Roadmap), published in January 2006.[5] The Energy Sector Control Systems Working Group, which recently formed under CIPAC, will further drive implementation of the Roadmap.[6] Also, eight new standards specific to cyber security in the Electricity Subsector are now being reviewed by the Federal Energy Regulatory Commission (FERC) (see attachment H).

The Energy Sector is involved in a considerable number of ongoing efforts to identify further gaps and vulnerabilities in cyber protection; these efforts include various risk and vulnerability assessments that are being conducted by owners and operators. Because energy systems are composed of many different types of assets, the "one size fits all" approach does not apply to the Energy Sector. DOE and DHS continue to work toward meeting the varying cyber security needs of this diverse infrastructure.

1.4 Sector Priorities

The Electricity and the Oil and Natural Gas Subsectors have in the past, and will continue to, collaborate in developing a unified set of priorities. The Energy Sector, in line with the four major categories of its security goals, has developed the following set of priorities.

1.4.1 Information Sharing and Communication

- Clearly define protocols for the protection and use of information shared between industry and Government.
- Actively exchange security-relevant information between public and private sector security partners.

1.4.2 Physical and Cyber Security

- Continue to conduct vulnerability assessments[7] to bolster security and preparedness in the industry.
- Implement protective measures that enhance preparedness, security, and resiliency by following sound risk-management principles.
- Secure control systems and related cyber networks.

---

5 See section 3 of this report.

6 See section 3 of this report.

7 Government energy security partners are working to coordinate such assessments with some programs like the Comprehensive Reviews and Site Assistance Visits, which are often carried out with the participation of more than one agency.

- Conduct comprehensive emergency, disaster, and continuity-of-business planning for all hazards to enhance reliability and emergency response.

1.4.3 Coordination and Planning

- Identify roles and responsibilities of Federal, State, local, tribal, and private sector security partners in critical infrastructure protection (CIP).
- Build on lessons learned to enhance crisis communication, coordination, and response.
- Establish an access system that allows private sector response personnel to access sensitive emergency sites and facilities for repairs.
- Map key sector interdependencies and initiate cooperation with other interdependent subsectors and sectors, such as Electricity, Transportation Systems, Communications, and Information Technology (IT).

1.4.4 Public Confidence

Building public confidence requires various protection activities, including all of the aforementioned sector priorities. In the summer of 2007, with the release of all the SSPs, including the Energy SSP, DHS launched a National Awareness Program that will serve a critical role in further educating industry personnel on the importance of protecting critical infrastructure, as well as building public confidence in national CIP efforts.

Section 2: Sector Programs, Activities, and Tools

2.1 CIKR Protection Programs and Initiatives

With voluntary cooperation and partnerships as a key cornerstone of its overall strategy, the Energy Sector already has more than 115 programs sponsored by dozens of public and private organizations that support the Sector's security goals.[8] These programs, identified during the Energy SSP development process and updated here, align with the four categories of security goals: (1) information sharing and communication, (2) physical and cyber security, (3) coordination and planning, and (4) public confidence. The Energy Sector will continue to evaluate and implement new protective measures as it assesses its security needs, develops programs, and identifies long-term solutions, including R&D needs.

2.1.1 Electricity Subsector

A number of electricity organizations have been very active in supporting voluntary cooperation within the Energy Sector. The following sections provide examples of the electricity-related organizations and activities that support the Energy Sector's security goals. For some cases, additional information is provided in attachment G: Energy Sector Protective Programs.

2.1.1.1 North American Electric Reliability Corporation

The North American Electric Reliability Corporation (NERC) is the officially designated Electric Reliability Organization (ERO) under the Energy Policy Act of 2000 and is composed of industry experts in the areas of cyber, physical, and operational security.

As such, NERC oversees the identification and collection of a considerable amount of information on the Electricity Subsector that is used to assess system protection and reliability. Various commercial entities have developed several databases that provide a substantial amount of information on the energy infrastructure.[9]

In addition, in 2007, NERC began enforcing and monitoring compliance with mandatory reliability standards that had been approved by FERC. Before March 2007, when FERC issued an order that approved 83 reliability standards, NERC had monitored compliance with the standards but did not have any authority to enforce them. NERC now has authority to penalize entities, including imposing fines (subject to FERC oversight), for failure to comply with mandatory reliability standards.

8 See chapter 5 and table 5.1 of the Energy SSP or attachment G of this report for a comprehensive review of protective programs.

9 See attachment H for a description of NERC's reliability standards with status and Sector goal categories.

2.1.1.2 Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC), in its role as the energy industry regulator, oversees NERC and establishes and enforces mandatory electricity reliability standards.

FERC took several measures last year toward enforcing compliance and addressing gaps in electricity reliability standards. In 2007, FERC accepted delegation agreements under Section 215 of the Federal Power Act between NERC and eight regional entities. The agreements delegated the regional entities with the authority to develop regional reliability standards for review and potential approval by FERC and also with the authority to enforce mandatory reliability standards approved by FERC, including the authority to impose penalties, subject to oversight by NERC and FERC.

In January 2008, FERC issued an order that approved eight CIP reliability standards that address the cyber security of control systems used to operate the Nation's bulk-power system. This order also approved a proposed implementation plan that specifies a schedule by which users, owners, and operators of the bulk-power system are to comply with the new CIP reliability standards. In addition, the order required modifications to the CIP standards to address specific concerns. The industry has started the process of developing these modifications.

In February 2008, FERC approved three new reliability standards concerning facility design, connections, and maintenance that address system operating limits for the bulk-power system in the planning and operation horizons, and it directed modifications to one of the new standards.

2.1.1.3 Edison Electric Institute

The Edison Electric Institute (EEI) is the association of U.S. shareholder-owned electric companies. Its members serve 95 percent of the ultimate customers in the shareholder-owned segment of the industry, representing about 70 percent of the entire U.S. electric power industry. EEI also represents more than 170 industry suppliers and related organizations.

In its leadership role, EEI provides advocacy, authoritative analysis, and critical industry data to its members, Congress, government agencies, the financial community, and other opinion-leader audiences. EEI provides forums for member company representatives to discuss issues and strategies to advance the industry and ensure its competitive position in a changing marketplace.

The EEI Security Committee, made up of physical and cyber security representatives from EEI member companies, provides an active forum for industry security professionals to share, develop, and benchmark effective security practices as well as exchange information on current and emerging threats and vulnerabilities. The Committee holds regular monthly conference calls (unless events warrant more frequent calls) and holds in-person meetings in the spring and fall. A joint electric and gas industry security conference, cosponsored by the EEI and American Gas Association (AGA) security committees, is held in conjunction with these in-person meetings. In the interest of sharing and developing effective security practices across all segments of the energy utility industry, this conference is open to non-EEI and non-AGA members.

EEI also hosts an annual mutual assistance conference and convenes a quarterly conference call to facilitate coordination of responses to all types of events. In addition, EEI has an active working group of about 200 business-continuity professionals from across the electric industry (including both EEI member and nonmember electric utilities). Since 2006, this group has organized four conferences on business continuity in the electric industry, including two specifically focused on planning for an influenza pandemic. At the most recent conference, a tabletop exercise of a pandemic scenario was conducted. To further enhance the industry's readiness for a pandemic, in early 2007, EEI hosted a special meeting for industry communications professionals to develop a crisis communications plan for an influenza pandemic.

The EEI Spare Transformer Equipment Program is an innovative approach to prepare for recovery from a physical attack on the utility infrastructure. About 50 utilities, together owning approximately 70 percent of the U.S. transmission assets, participate in this program. The program holds annual meetings and quarterly conference calls to discuss emergency planning and needs. The program was exercised in August 2007, and a second exercise is planned for August 2008.

2.1.1.4 American Public Power Association (APPA)

The American Public Power Association (APPA) is the service organization for the Nation's more than 2,000 community-owned electric utilities that serve more than 45 million Americans. It was created in 1940 as a nonprofit, nonpartisan organization.

APPA has taken a leadership role over the years to help educate, inform, and assist its members in various aspects of utility operations, including the security of their assets and the reliable delivery of service to their community. APPA staff members have been active participants in virtually all NERC and DOE activities, including the NERC CIP Committee (CIPC), and they will continue to be whenever DOE or DHS offers a reasonable opportunity.

APPA has identified effective security practices that can be shared with all municipal utilities so they can learn from the leaders in this process. It produced a Reliable Public Power Provider (RP3) Program guidebook on effective security practices in 2007, which highlighted the disaster management and preparation manuals from several utilities. APPA has also encouraged all municipal utilities to sign a mutual aid agreement for securing mutual help among utilities during an emergency. Over the past eight years, more than 700 utilities have signed this agreement, and those that were affected when the United States was struck by severe hurricanes, such as Katrina, Francis, Charlie, and Rita, reaped immense benefits.

Other APPA initiatives include its guidebook on distribution circuit inspections, produced in 2004, which helps utilities in the early detection of distribution system problems. In 2006, APPA produced a guidebook to help its members deal with FEMA in the aftermath of major disasters.

Overall, APPA continues to work with its members to improve and adapt to the changing needs of the electric utility world in the areas of safety, reliability, and security.

2.1.1.5 National Rural Electric Cooperative Association

The National Rural Electric Cooperative Association (NRECA) is a nonprofit service organization representing about 930 nonprofit, member-owned, rural electric cooperatives. Most are distribution cooperatives that provide retail electric service to more than 37 million consumers in 47 States. NRECA members also include about 65 generation and transmission cooperatives. Kilowatt-hour sales by rural electric cooperatives account for about 10 percent of total electricity sales in the United States.

About two thirds of NRECA's electric cooperative members receive financing from the Rural Utilities Service (RUS) section of the U.S. Department of Agriculture (USDA). As recipients of this financing, these cooperatives must comply with the RUS emergency restoration plan (ERP) regulation that requires them to perform a vulnerability and risk assessment, effectively develop a disaster/business-continuity plan, and practice this plan annually.

NRECA also held a series of workshops at eight locations nationwide that focused on managing physical and cyber security for the electric cooperative infrastructure. Attended by about 1,000 cooperative representatives, the workshops provided expert information on the RUS ERP regulations, NERC security guidelines, and other effective CIP security practices. In addition, NRECA distributed its CD-ROM, *IT Recovery Plan for Electric Co-ops,* to attendees. The plan guides cooperatives to develop a disaster and business-continuity plan for their IT and business system assets.

Continuing efforts include numerous Web conferences and conference calls with member cooperatives on a variety of topics, including how to conduct a tabletop drill and how to plan for disaster and business-continuity issues related to the threat from a possible avian flu pandemic. NRECA also created a Reliability Task Force of member cooperatives that focuses on reliability issues, including CIP. NRECA has separate LISTSERVs (electronic mailing list software application) focused on reliability, IT, and security issues that give electric cooperatives the opportunity to quickly communicate with each other on these issues.

NRECA communicates with its member cooperatives on a continuing basis through emails, phone calls, weekly and monthly publications, and other R&D products through its Cooperative Research Network. This effort ensures that members are kept up to date on the important and constantly changing issues related to safety, reliability, CIP, and security.

2.1.1.6 Electric Power Administrations

The electric power administrations — including the Western Area Power Administration, Bonneville Power Administration (BPA), Tennessee Valley Authority (TVA), and Southeastern Power Administration — deliver power to distribution companies and for direct use. Recipients include municipalities, cooperatives, public utility and irrigation districts, Federal and State agencies, Native American tribal projects, and investor-owned utilities. The distribution organizations, in turn, provide retail electric service to millions of consumers in their regions.

Reliability is an important focus of the power administrations; this includes the protection of assets and restoration and recovery from energy-related incidents and events.

2.1.1.6.1 Western Area Power Administration (Western)

Western, under DOE, markets and transmits wholesale electric power from 56 Federal hydropower plants and one coal-fired plant. Western sells about 40 percent of regional hydroelectric generation in a service area that covers 1.3 million square miles in 15 States. To provide this reliable electric power to most of the western half of the United States, Western markets and transmits about 10,000 megawatts of hydropower across an integrated 17,000-circuit-mile, high-voltage transmission system. The following list highlights some Western activities currently under way.

- Western is implementing the Homeland Security Presidential Directive 12 (HSPD-12), mandatory, U.S.-Government-wide standard for secure and reliable forms of identification for Federal employees and contractors. A card verifying an employee's identity will be used for accessing all Federal facilities and IT systems. The standard will allow interoperable use of identity credentials, allowing physical and logical access to Federal Government locations and systems.

- In accordance with standards established by NERC in 2006, and specifically with regard to cyber security, Western is conducting an identity verification and a criminal check of all employees in identified groups, at a minimum of once every seven years.

- Western's Human Resources Office has begun accounting for the criminal checks and identification verifications of Federal employees conducted within the last seven years. As it progresses in the assessment process, Western will have updated data on all active Federal employees subject to this requirement.

- In May 2008, Western made it a requirement that all support service contractors undergo a background investigation. A support service contractor is a contractor who needs physical and logical access to Western facilities. This requirement will be incorporated in all of Western's support service contracts.

- Western hired full-time security specialists in each region to implement security policies and procedures across its facilities.

- Western is continuing to conduct security assessments, budget, and implement security upgrades at its identified sites.

2.1.1.6.2 Tennessee Valley Authority

The TVA, the Nation's largest public power provider, is wholly owned by the U.S. Government. It was established by Congress in 1933 to provide for river navigation, flood control, and agricultural and industrial development and to promote the use of electric power in the Tennessee Valley region. TVA's service territory includes most of Tennessee and parts of Alabama, Georgia, Kentucky, Mississippi, North Carolina, and Virginia. This area covers 80,000 square miles and has a population of more than 8.7 million. TVA sells electricity to 158 power distributor customers and 62 directly served industries and federal agencies.

2.1.1.6.3 Bonneville Power Administration

The BPA provides about half of the electricity used in the Northwest and operates over three-fourths of the region's high-voltage transmission lines. BPA's service territory covers all of Washington, Oregon, Idaho, and western Montana, as well as small contiguous portions of California, Nevada, Utah, Wyoming, and eastern Montana. BPA's wholesale customers include public utilities, public utility districts, municipal districts, public cooperatives, some investor-owned utilities, and a few large industries, such as aluminum companies.

2.1.1.7 USDA Rural Development Electric Programs

The USDA's rural development electric programs provide reliable and affordable electricity for rural residents. The programs provide capital to upgrade, expand, maintain, and replace America's vast rural electric infrastructure. Under the authority of the Rural Electrification Act of 1936, the programs make direct loans and loan guarantees to electric utilities to serve customers in rural areas.

The loans and loan guarantees finance new construction and upgrades of electric distribution, transmission, and generation facilities and contribute toward improving electric service in rural areas, demand side management, energy conservation programs, and on-grid and off-grid renewable energy systems. Loans are made available to entities that meet retail electric service needs or the power needs of distribution borrowers in rural areas.

Through these electric programs, the Federal Government is the majority note holder for about 700 electric system borrowers in 46 States. Under the programs, these distribution companies are required to do contingency emergency restoration planning and vulnerability assessments.

2.1.2 Oil and Natural Gas Subsector

2.1.2.2 Petroleum Refining Subsector

2.1.2.2.1 National Petrochemical and Refiners Association

The National Petroleum and Refiners Association (NPRA) has more than 400 member companies, including virtually all U.S. refiners and petrochemical manufacturers, and many of their suppliers and vendors. This membership includes 49 petroleum refining companies representing more than 95 percent of the refining capacity in the United States.

NPRA members consider maintaining the security of refining and petrochemical manufacturing facilities as a priority, and they commit substantial resources to the cause. NPRA has a very active Security Committee, with representatives from 30 large and small refiners and petrochemical manufacturers. This committee meets four to six times a year, while subcommittees and working groups of the Security Committee meet more frequently as needed.

As part of its outreach efforts, NPRA has published a white paper entitled *Hurricane Security Operations,* with recommendations for security planning in the event of a hurricane. Also, with the assistance of DHS, NPRA joined with the American Petroleum Institute (API) to produce *Security Vulnerability Assessment Methodology.* Both of these publications are available for free at NPRA's Web site at http://www.npra.org/publications/general. Moreover, the association has conducted or helped conduct numerous workshops and seminars on security practices and procedures, where industry personnel from the largest to the smallest companies have shared effective security practices.

NPRA works closely with both DOE and DHS as part of the "public/private partnership" and plans to continue this relationship in the future. NPRA facility security officers appreciate DOE and DHS efforts to keep them apprised of threats to the petroleum industry. The refining industry also often cooperates with State, local, tribal, and Territorial security partners in training activities, recognizing the benefits of such efforts.

Since September 11, 2001, the refining and petrochemical industries have been active in implementing far-reaching facility security measures to address any potential new threats. To the best of NPRA's knowledge, all of its members' manufacturing facilities have undertaken risk and vulnerability assessments of their assets, and many have been actively involved in developing and exercising business-continuity plans. (NPRA, as an organization, has its own such plan.) This industry has also developed close working relationships with key Federal agencies and State and local law enforcement offices to exchange information on maintaining infrastructure security. NPRA has held joint training exercises simulating actual terrorist attacks and developed educational programs involving Federal and State Government officials who have security expertise.

Pursuant to the Chemical Facility Anti-Terrorism Standards Act of 2006 (CFATS Act), refiners and petrochemical manufacturers have registered their facilities with DHS, conducted "top screen" assessments, and invited Federal Protective Service chemical regulation inspectors to their facilities. To keep up to date with all CFATS Act requirements as announced by DHS, NPRA members have participated in conferences and workshops.

Facilities subject to the requirements of the Maritime Transportation Security Act (MTSA) have conducted detailed vulnerability assessments of their facilities, submitted facility security plans to the U.S. Coast Guard (USCG), and conducted on-site annual audits to ensure continued compliance. MTSA-covered companies are enrolling their employees who require unescorted access to secure areas in the Transportation Worker Identification Credentials (TWIC) Program at Transportation Security Administration centers.

Because they are manufacturers who acquire raw materials and turn them into products that must reach consumers, NPRA members are keenly aware of their business vulnerabilities. For example, NPRA has a Cyber Security Subcommittee to advise and assist its members on matters pertaining to cyber security and cyber terrorism that target business systems and/or control systems in the refining and petrochemical industries.

Finally, NPRA effectively communicates with it members on pertinent security issues. It encourages its members to use the Homeland Security Information Network for the oil and natural gas sector (HSIN-ONG) and chemical sector (HSIN-CS). It also publishes *Security Watch,* a weekly digest of important security-related events, announcements, and background stories from Government and industry.

2.1.2.2.2 American Petroleum Institute

The American Petroleum Institute (API) represents all aspects of America's oil and natural gas industry, with 400 corporate members — from the largest major oil company to the smallest independent companies. As the largest trade organization in the Energy Sector, API includes producers, refiners, suppliers, pipeline operators, and marine transporters, as well as service and supply companies that support all segments of the industry.

API has been very active in energy security, resiliency, and restoration activities. API's Security Committee meets regularly with representatives from DOE, DHS, and the U.S. Coast Guard to discuss issues of mutual concern. The following are examples of security-related efforts undertaken since June 2007.

API has been participating in CIP briefings and discussions through the CIPAC Joint Energy Working Group, which coordinates CIKR protection programs and works closely with the Oil and Natural Gas SCC and the Energy GCC. The briefings and discussions serve as a forum to outline and discuss the progress of the partnership. Some specific areas addressed during the year include pending chemical security regulations, implementation of the TWIC Program, and pandemic planning.

API has also been active in DHS's HSIN-ONG, which serves as the leading mechanism for reporting industry incidents and disseminating information. This working group strives to hold monthly teleconferences to make this system valuable for the industry. (The system replaced the Energy-ISAC early in 2007 and is free to the industry.) API is also involved in the Information Sharing and Analysis Center (ISAC) Council, a collection of critical infrastructure ISACs that share information and leverage opportunities. The council holds a number of meetings and has a number of conference calls and classified briefings each year, averaging two contacts a month.

API has made an extensive effort to address the cyber security of the petroleum industry. It participated in DOE's Conference on Cyber Security Research Needs for Open Science in 2007, which was held to help identify research needs and opportunities. The conference focused on developing ways to prioritize future research in order to secure control systems in the Energy Sector.

API's Information Management and Technology Program completed the second industry IT security benchmark survey in the last quarter of 2007. The survey provides a comprehensive review and quantitative assessment of company security programs, with a focus on "due care" requirements and a rolling database of security programs and compliance initiatives. Results of the survey are being analyzed to drive 2008 joint projects and meeting agendas, as well as to develop industry messages about IT security in the industry.

2.1.2.3 Natural Gas Subsector

The American Gas Association (AGA) represents local energy utility companies that deliver 92 percent of all natural gas provided by the Nation's natural gas utilities to more than 64 million homes, businesses, and industries throughout the United States.

The AGA Natural Gas Security Committee (NGSC) covers 65 gas utility and transmission member-companies. More than 100 committee members represent natural gas distribution, transmission, and combination electric/gas companies. NGSC serves the following functions:

- Provides a forum for the identification, development, and communication of innovative and cost-effective security solutions for the natural gas industry.
- Provides insight on physical infrastructure security-related issues through AGA's operating, government relations, and regulatory affairs sections.
- Investigates new technologies related to infrastructure protection.
- Sponsors programs, papers, and presentations at technical symposiums in the energy industry.
- Develops and publishes committee reports and technical papers and provides and encourages liaisons with appropriate national and international industry groups,

professional associations, and other committees to exchange information and technical help on infrastructure protection.

- Establishes a common ground for the promotion and development of viable external relationships with governmental agencies and public law enforcement and emergency response organizations.

The AGA has well-established mechanisms for communicating with its members:

- The NGSC roster serves as a conduit for security-related information pertinent to natural gas utility and transmission operations in the private and public sectors.

- A comprehensive roster of AGA member-company executives (which is in addition to the NGSC roster) is the conduit for time-sensitive security-related government advisories.

- Monthly security update calls are held in conjunction with intelligence conference call briefings by DHS HITRAC and the U.S. Computer Emergency Readiness Team (US-CERT).

- It holds semiannual committee meetings.

- Jointly with EEI, it holds semiannual security conferences for gas and electric utilities

The AGA has been actively involved in security-related initiatives for the Natural Gas Subsector. Some highlights are described below:

- The industry-developed publication, *Security Guidelines: Natural Gas Industry, Transmission and Distribution,* has served the industry well with regard to advancing its security initiatives. The version published in 2002 has been accepted by the industry's governmental security partners and referenced in numerous government documents, including the applicable SSPs from both DOE and the DHS Transportation Security Administration (TSA).

- Products and opportunities provided by NGSC include a membership skills database, *Contract Worker Background Screening Guidelines,* a cyber security benchmarking survey, roundtable discussions for sharing information on industry practices, a Cyber Security Task Group, and a physical security survey. AGA and industry representatives helped developed and are participating in the implementation of DOE's Roadmap, and they also participate in and lead efforts for the Oil and Natural Gas SCC. AGA members also invest significant resources to ensure the effective implementation of access credentialing, TWIC, security metrics, the National Response Framework (NRF), and pandemic planning, and other activities.

Restoration and recovery are also an important focus of this Subsector, similar to the Electricity Subsector:

- The AGA Natural Gas Mutual Aid Resource Center (NG MARC) helps gas utilities quickly and effectively attain the personpower and materials they need to efficiently restore service. A culmination of efforts of the utility community, it gives users broad access to utility companies throughout the Nation through searchable lists of emergency contact information, field capabilities, and other resources available for mutual assistance.
  - The AGA Mutual Aid Database is populated with emergency contact and other key information pertaining to mutual aid for more than 70 AGA member-companies. This tool also provides references for developing mutual aid agreements (e.g., agreement template, task order template, assistance guidelines, information on lessons learned) between parties.
  - The AGA developed the National Natural Gas Operations Assistance Program to govern the provision of mutual assistance between gas utilities in the event a man-made or natural disaster would require the dedication of response/recovery/restoration resources outside the limits of existing State and regional mutual aid programs.
- There are natural gas regional mutual aid and planning organizations and arrangements outside the AGA. These include Mid-Atlantic Regional Planning, Ohio/Kentucky Gas Association Supply Contingency Planning, Pacific Northwest Regional Economic Conference, Northwest Mutual Aid Agreement Group, Northeast Gas Association Operations Emergency Mutual Assistance Plan, Southern Gas Association Mutual Assistance, and Western Region Mutual Assistance Agreement.
- AGA and industry representatives continue to be active contributors to DOE regional planning studies.
- AGA and industry representatives actively participate in interdependency initiatives coordinated by Federal and State governments.

2.1.3 Pipeline Transportation[10]

In the U.S. Department of Transportation (DOT), the Pipeline and Hazardous Materials Safety Administration (PHMSA), acting through the Office of Pipeline Safety (OPS), administers DOT's national regulatory program to ensure the safe transportation of natural gas, petroleum, and other hazardous materials by pipeline. The OPS develops regulations for and other approaches to risk management in order to ensure safety in the design, construction, testing, operation, maintenance, and emergency response of pipeline facilities. The entire pipeline safety program has been funded since 1986 by a user fee assessed on a per-mile basis on each pipeline operator that is regulated by OPS.

10 Attachment I provides a discussion of the DHS pipelines program at TSA.

One of PHMSA's programs defines critical pipeline facilities, identifies appropriate countermeasures for protecting them, and explains how PHMSA plans to verify that operators have taken appropriate action to implement satisfactory security procedures and plans.

2.1.4 Maritime Transportation

2.1.4.1 Committee on the Marine Transportation System

In July 2006, the Secretary of Transportation announced the appointment of the first Director of the Executive Secretariat to the Committee on the Marine Transportation System (CMTS). The CMTS was established by the President's Ocean Action Plan in December 2004 to create a partnership of Federal agencies with responsibility for the Marine Transportation System (MTS): waterways, ports, and their intermodal connections. The goal was for the CMTS to ensure the development and implementation of national MTS policies consistent with the Nation's needs and to report to the President its views and recommendations for improving the MTS. The CMTS is chaired by the Secretary of the Department of Transportation and composed of 18 Cabinet-level departments, independent federal agencies, and White House offices. The CMTS has called for several interagency action teams to address issues that affect or could improve the MTS, including the development of a national strategy for the MTS, an assessment of the MTS, Federal integration and coordination of navigation technology, Federal collection of maritime data, and financing of the MTS infrastructure.

2.1.4.2 Maritime Transportation Security Act

The security of all U.S. ports, waterfront facilities, and vessels, including those involved with the Natural gas and Oil Subsector, is regulated by the Maritime Transportation Security Act (MTSA) and implemented through U.S. Coast Guard (USCG) regulations. The MTSA details the requirements for facility security assessments (FSAs) and facility security plans (FSPs). Key elements of the MTSA include the following:

- Maritime security plans on national, area, vessel, and facility levels.
- Incident response plans on vessel and facility levels (which may be incorporated into security plans).

Thus, a refinery that receives or ships bulk shipments via water vessels, including via a pipeline to the waterfront, must meet MTSA requirements.

Under the MTSA, energy facilities must complete periodic vulnerability assessments or FSAs and have FSPs. While these requirements impact refineries, the USCG does not maintain a list of refineries that need to be MTSA-compliant. Instead, it has a list of 852 facilities that handle bulk oil and have water access in the United States. The list includes refineries, petroleum terminals, power plants operating on fuel oil, and other water-based facilities. Thus the MTSA impacts a

number of different types of energy facilities. An initial secondary analysis of the MTSA data indicates that about 81 of the facilities in the USCG list are estimated to, in fact, be refineries. In addition, it is estimated that 66 of the refineries operate in the United States but do not have to be MTSA-compliant. The USCG, during its next round of assessments, is introducing facility coding that will allow for a clearer understanding of the assets covered.

2.1.5 Offshore Mineral Resources

The U.S. Department of the Interior's (DOI's) Minerals Management Service (MMS) manages the Nation's natural gas, oil, and mineral resources off America's coast on the Outer Continental Shelf (OCS). MMS reports on production status during energy emergencies that affect offshore oil and gas production. These offshore assets produce 27 percent of U.S. domestic oil and about 15 percent of its natural gas.

Energy exploration and development in the deep water of the Gulf of Mexico are a key source of new oil and gas in the United States. Most of the energy discoveries of recent years have been found in the deep-water Gulf, with more than 50 percent of the Gulf's 8,000 active leases being there. More than 980 exploration wells have been drilled in the deep-water Gulf since 1995, and at least 126 deep-water discoveries have been announced since then. Forty deep-water Gulf projects were active as of June 2, 2008. For 2006, deep-water Gulf production totaled 342,531,863 barrels of oil and 1,094, 672,953 million cubic feet (Mcf) of natural gas. These numbers represents about 72 percent of total Gulf oil production and about 38 percent of total Gulf gas production. In addition, with recent higher energy prices, exploration and production are increasing in the Continental United States, including the Eastern Great Basin, Powder River Basin, Uinta-Piceance Basin, and Southwestern Wyoming. DOE coordinates with the MMS on the safety and security of OCS energy production. DOE also coordinates with the U.S. Geological Survey in DOI regarding coal mines, geothermal production areas, and power plant siting. Finally, DOE's power marketing administrations coordinate their power generation and river operations with DOI's Bureau of Reclamation (BOR) hydrogeneration projects.

2.1.6 Storage Operations

The International Liquid Terminals Association (ILTA) addresses a broad regulatory agenda, including the regulation of energy, through its Environmental, Health, Safety, and Security Committee, which has 80 corporate members. Within this construct, ILTA has an active Security Working Group. The group has been addressing a number of issues of concern to its members with regard to the CFATS Act and the TWIC Program and their applicability to MTSA-covered facilities.

2.1.7 International Activities

2.1.7.1 U.S. Department of Energy

DOE, in cooperation with DHS and the U.S. Department of State, participated in a number of international activities in cooperation with foreign energy security partners.

The United States depends on and is a part of the global energy market. It is in our Nation's interest, as well as our energy-producing allies' interest, to improve the security of critical energy infrastructure located outside the United States to help ensure the uninterrupted flow of energy supplies from abroad to the United States. Energy security is a national security imperative and one of DOE's five strategic themes. Earlier this year, DOE-OE, which is the principal DOE organization for implementing this strategy, established an international team within its Office of Infrastructure Security and Energy Restoration (ISER).

DOE is leveraging its own Energy Sector expertise and that of its Energy Sector security partners in government and the private sector to develop and execute packages for assessing energy infrastructure systems. These are designed to enhance U.S. efforts to identify, assess, and help key allies mitigate the risks to critical Energy Sector assets located outside the United States. Current international activities include the following:

- ISER, in partnership with the U.S. Department of State and DHS, is helping three countries improve their critical energy infrastructure security.
- The ISER international team is coordinating with DHS to develop the Critical Foreign Dependencies Initiative, the goal of which is to identify and assess overseas critical infrastructures in all sectors.
- A strategy is being developed for managing and funding DOE's overseas presence.
- DOE and the U.S. Department of Defense (DoD) are working on developing and implementing a ground-breaking energy security strategic plan.
- DOE and DOD are determining the energy security requirements of DoD combatant commands, beginning with EUCOM and AFRICOM.
- DOE is cooperating with Natural Resources Canada under the Security Partnership for North America.

2.1.7.2 Cross-border Electricity (Presidential Permits)

OE issues Presidential permits to construct, operate, maintain, and connect electric transmission facilities at the international borders with Canada and Mexico. OE also authorizes electricity exports, contributing to the U.S. economy. During the fourth quarter of 2007, power marketers

sold approximately $195 million in electricity. Higher amounts of electricity move north during the winter; in the first quarter of 2008, electricity sales were approximately $344 million.

About 120 transmission lines cross the borders. They vary in size from small distribution lines, which may provide electricity to single homes or small communities, to a 765-kV transmission line that originates in Quebec and transmits hydro-generated electricity to New England. The international transmission facilities owned by the BPA in the Northwest provide a critical path to the California market. At the U.S. border with Mexico, there are major interconnections between California and Baja California, Mexico, that connect to Comisión Federal de Electricidad (CFE), the national electricity company of Mexico. There are also two large natural-gas-fired power plants near Mexicali, Mexico, that connect directly to the electricity delivery system of California and are not otherwise interconnected with CFE. While imported electricity makes up only about 2 percent of total domestic consumption, the contribution of imports is much more significant on a regional basis; imports serve about 12 percent of the New England load.

The North American interconnected transmission system has allowed the United States to supply electricity to Canada and Mexico during several of their energy emergencies, contributing to the resiliency of the supply in each country. For example, in 1998, the United States responded to Canada's need, supplying electricity when severe ice storms toppled a portion of Canada's interprovincial transmission facilities. In a similar way, the interconnected transmission system contributes to the resiliency of the U.S. electricity supply.

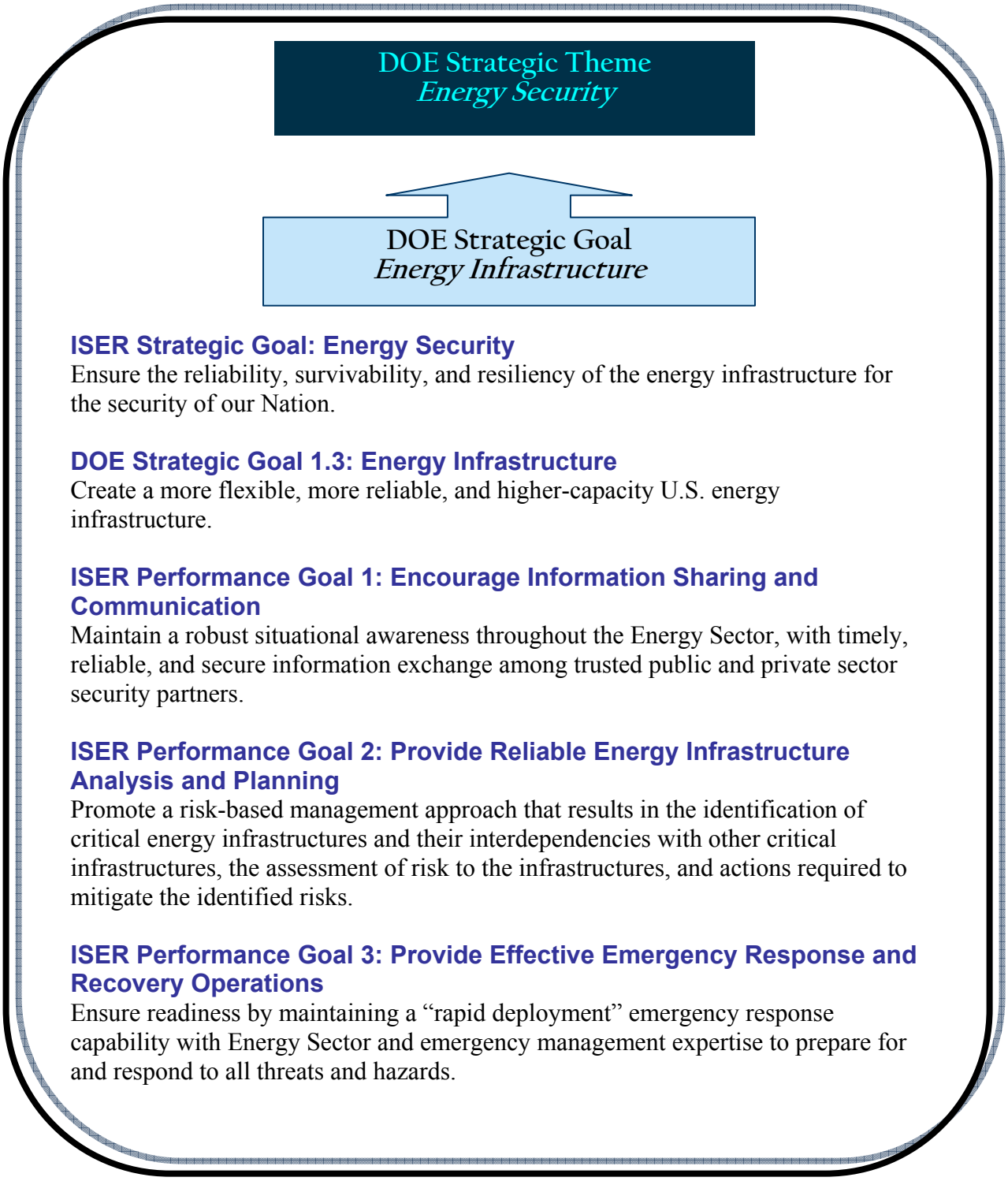
2.1.7.3 G-8 and Asia Pacific Economic Cooperation

Energy security has been a focus of G-8 and Asia Pacific Economic Cooperation (APEC) activities. DOE, in cooperation with DHS and the State Department, developed and completed a questionnaire to assess ongoing efforts in member countries. The Energy SSP (redacted) has been shared with participants in both G-8 and APEC groups.

2.1.8 ISER Strategic Plan

ISER, an office in DOE-OE, is responsible for leading DOE's infrastructure and preparedness planning, analysis, and operational efforts and for developing strategies, policies, and plans to successfully execute Energy Sector responsibilities. Its mission is to lead the national effort to enhance energy infrastructure security and reliability. The ISER Strategic Plan summarizes an approach for enhancing risk management decisions at all levels to ensure that critical infrastructure is available and that operational capabilities are in place to respond to and recover from major disasters (figure 2-1).

The ISER Strategic Plan tracks with two DOE strategic themes: energy security and management excellence. DOE's strategy is to nurture the development of an organization, culture, and management process that will make the Energy Sector resilient. Teamwork is vital. Security partners throughout the Federal, State, tribal, and local governments and the private sector, as well as law enforcement officials, first responders, international partners, and others, must



ISER Strategic Goal: Energy Security

Ensure the reliability, survivability, and resiliency of the energy infrastructure for the security of our Nation.

DOE Strategic Goal 1.3: Energy Infrastructure

Create a more flexible, more reliable, and higher-capacity U.S. energy infrastructure.

ISER Performance Goal 1: Encourage Information Sharing and Communication

Maintain a robust situational awareness throughout the Energy Sector, with timely, reliable, and secure information exchange among trusted public and private sector security partners.

ISER Performance Goal 2: Provide Reliable Energy Infrastructure Analysis and Planning

Promote a risk-based management approach that results in the identification of critical energy infrastructures and their interdependencies with other critical infrastructures, the assessment of risk to the infrastructures, and actions required to mitigate the identified risks.

ISER Performance Goal 3: Provide Effective Emergency Response and Recovery Operations

Ensure readiness by maintaining a "rapid deployment" emergency response capability with Energy Sector and emergency management expertise to prepare for and respond to all threats and hazards.

Figure 2-1: ISER Strategic Plan

effectively work together to attain ISER's vision of a secure, reliable, and resilient energy infrastructure."

The ISER Strategic Plan relates closely to the ESSP and contributes to the DOE-led energy security partnership under the NIPP in addressing the complex issues associated with energy reliability, survivability, and resiliency. The plan supports implementation of the vision, goals, and milestones in the Energy SSP.

ISER is responsible for coordinating DOE's response to energy emergencies and for supporting the national homeland security policy, which requires DOE to secure energy infrastructure and assist State and local governments with energy assurance planning and preparing for disruptions responses to disruptions.

ISER organization addresses two needs: (1) infrastructure analysis and planning and (2) infrastructure operations and support. ISER staff members are located at DOE headquarters in Washington, D.C.; at the National Energy Technology Laboratory (NETL) in Morgantown, West Virginia; and at the HAMMER training and Education Center in Richland, Washington.

Through its work, ISER actively collaborates with other DOE offices, Federal agencies, State and local governments, industry, and foreign governments. These activities include:

- Supporting State and local organizations in creating energy assurance planning tools for State and local energy officials, State governors, and State legislatures and holding energy emergency exercises for State and local government officials to test those plans.

- Creating the Energy SSP annex to the NIPP. This plan was prepared through work with the Electricity SCC, Oil and Natural Gas SCC, and Energy GCC, as well as other government and industry partners.

- Coordinating with FEMA to prepare for and respond to energy emergencies. When not responding to emergencies, the ISER works with FEMA on determining proper response procedures and informs FEMA about areas in which ISER and DOE can provide expertise and assistance. During a large-scale energy emergency, ISER staff will deploy to the affected region to assist in the recovery efforts.

- Working with Energy Sector experts and Energy Sector security partners in government and the private sector to develop and execute a scalable suite of energy infrastructure support products. These are designed to enhance U.S. efforts to identify, assess, and help key allies mitigate the risks to critical energy sector assets located outside the United States.

2.1.9 DHS Infrastructure Protection Program

DHS has several programs related to energy security. Energy Sector security partners are participating and cooperating with DHS in these programs.

2.1.9.1 Constellation/Automated Critical Asset Management System

The Constellation/Automated Critical Asset Management System (C/ACAMS) is a secure, Web-based portal designed to help State and local first responders, emergency managers, and homeland security officials collect and organize CIKR asset data as part of a comprehensive CIKR protection program. The program was developed in partnership with the Los Angeles Police Department's Operation Archangel and the FEMA National Preparedness Directorate. It is provided free for State and local use and is available at www.dhs.gov/acams.

C/ACAMS provides comprehensive infrastructure inventory management and vulnerability assessment tools, role-based access, standard and customized reports, asset manager questionnaires, buffer zone protection plan development tools, a CIKR asset taxonomy classification capability, an electronic CIKR reference library, mapping and geospatial functionality through the Integrated Common Analytical Viewer (iCAV), and live law enforcement and counterterrorism news feeds and public disclosure protections through the DHS Protected Critical Infrastructure Information (PCII) Program. Some States and local governments are currently participating in the program.

2.1.9.2 Infrastructure Information Collection Division

The Infrastructure Information Collection Division (IICD) leads DHS efforts to acquire and provide standardized, relevant, and customer-focused infrastructure data to homeland security partners. In doing so, IICD aims to create more relevant infrastructure information; enable timely and actionable decisions to protect, secure, analyze, and restore the Nation's infrastructure; and facilitate a persistent awareness of the Nation's infrastructure.

To support DHS, IICD collects, catalogs, and maintains standardized and quantifiable infrastructure information to enable national risk management, infrastructure protection, and incident management. IICD also supports the implementation of automated tools for risk and vulnerability self-assessments, if needed.

2.1.9.3 Integrated Common Analytical Viewer

iCAV is a secure, Web-based geospatial analytical and situational awareness system, consisting of government-owned and licensed data, imagery, and dynamic mission-specific information feeds (on threats, weather, situations, etc.). iCAV provides a geospatial context for a wide variety of information systems, fusing information and providing for situational awareness by tracking real-time events. This fusion provides Federal, State, and local jurisdictions and the private sector with a rapid, common understanding of the relationships between events to support coordinated preparedness, response, and recovery activities. In providing a robust data integration and management platform, iCAV can make various data sets available to homeland security partners.

2.1.9.4 Protected Critical Infrastructure Information Program

The PCII Program enables the secure collection and sharing of information by protecting critical infrastructure information (CII) that is voluntarily submitted to DHS and meets certain requirements from public disclosure. Once the information has been validated as PCII, it is protected from Federal, State, and local disclosure laws and from use in civil litigation. The PCII Program works with various government partners to integrate these protections into their data-collection processes. This system offers a way for CII to flow to analysts and homeland security partners, while the CII owners and operators are assured that the information they provide is protected. The Web site www.dhs.gov/pcii has more information.

2.1.9.5 Protective Security Advisors

Protective Security Advisors (PSAs) represent DHS and the DHS Office of Infrastructure Protection (IP) in local communities throughout the United States. PSAs work with State Homeland Security Advisor (HSA) offices, serving as liaisons between DHS and Federal, State, Territorial, tribal, and local entities and the private sector and also acting as DHS on-site specialists with regard to critical infrastructure and vulnerability assessments. During natural disasters and contingency events, PSAs work in State and local emergency operations centers (EOCs) and often provide expertise and support to IP's Infrastructure Liaison Cell, working to support the Principal Federal Official (PFO) and Federal Coordinating Officer (FCO) responsible for domestic incident management. In addition, PSAs provide support to officials responsible for special events planning and exercises, and they provide real-time information on facility significance and protective measures to facility owners and operators, as well as State and local representatives.

This DHS program has placed 68 PSAs around the country to help communities better protect the Nation's critical assets (figure 2-2). These advisors represent DHS's principal outreach capability. They visit and get to know State, local, tribal, and Territorial officials and asset owners and operators in the Energy Sector. As of May 2008, PSAs visited 495 energy assets In addition, 33 of these assets have participated in the DHS Enhanced CIP (ECIP) initiative. The purpose of ECIP visits is to begin a dialogue between DHS and the asset about the security of the asset. The questionnaire is filled out by the PSA, with inputs from representatives of the asset.

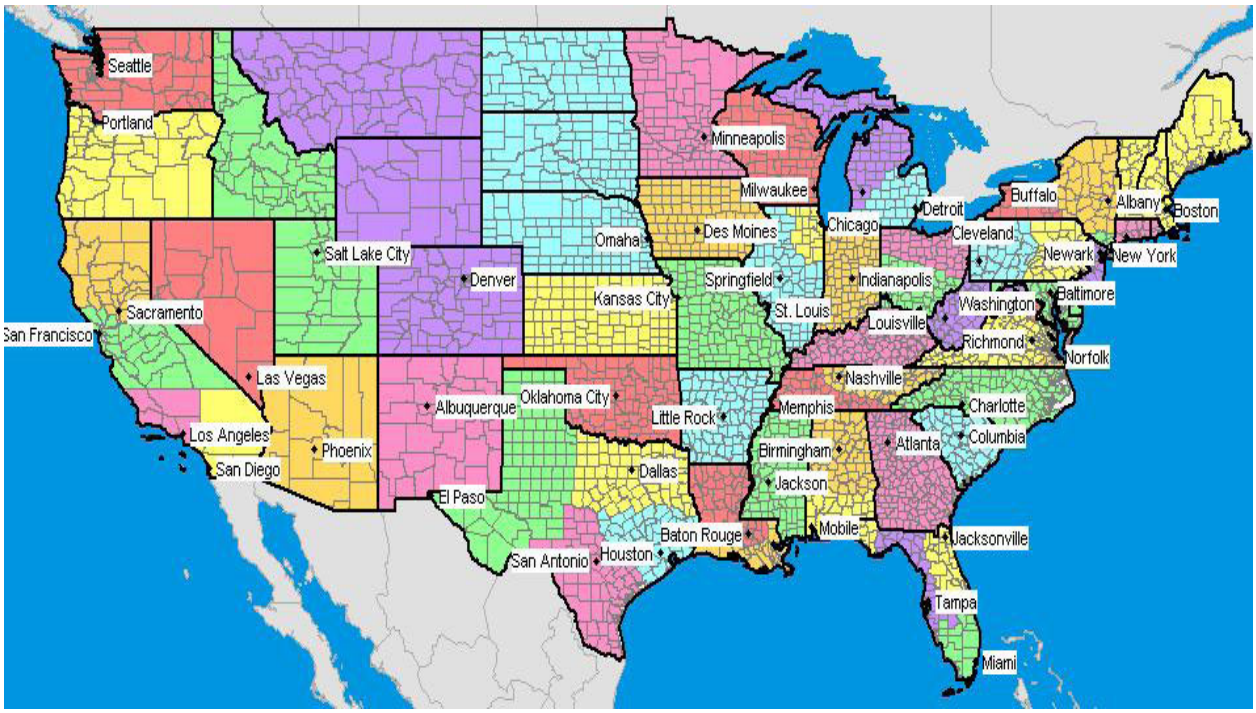


Figure 2-2: DHS PSA Districts

2.1.9.6 Buffer Zone Protection Program

DHS's Buffer Zone Protection Program (BZPP) provides grants to State and local entities to build capabilities at their level to prevent and protect CIKR from terrorist attacks. By doing this, the BZPP supports the implementation of the goals outlined in the NIPP and State/Urban Area Homeland Security Strategies (particularly in the prevention and protection mission areas) and addresses many national infrastructure protection priorities and related target capabilities.

The program helps to implement buffer zone plans (BZPs) by providing funds to support planning and equipment acquisition. A portion of these funds have supported the protection of the highest-priority CIKR assets across certain targeted sectors, including energy assets.

In fiscal year 2007 (FY 2007), $48,500,000 was to be awarded. Table 2-1 lists energy assets at which BZPP grants for energy were offered between May 2007 and May 2008.

Table 2-1: Recipients of BZPP Grants, May 2007–May 2008

Name	City	County	State	BZPP Grant
ExxonMobil Torrance Refinery	Torrance	Los Angeles	CA	5/8/2007
ConocoPhillips Wilmington Refinery	Wilmington	Los Angeles	CA	5/14/2007
US Los Angeles Refinery (LAR)	Los Angeles	Los Angeles	CA	5/14/2007
Sunoco Toledo Refinery	Oregon	Lucas	OH	5/30/2007
Sunoco Philadelphia R&M Refinery	Philadelphia	Philadelphia	PA	7/10/2007
Valero Refining Memphis Refinery	Memphis	Shelby	TN	10/9/2007
ConocoPhillips Alliance Refinery - Belle Chasse	Belle Chasse	Plaquemines Parish	LA	10/28/2007
William R. Gianelli Pumping-Generating Plant	Gustine	Merced	CA	3/10/2008
Colonial Pipeline Pasadena Station	Pasadena	Harris	TX	4/7/2008
Pearblossom Pumping Plant	Pearblossom	Los Angeles	CA	4/28/2008
Castaic Powerplant	Castaic	Los Angeles	CA	4/29/2008
Devon Bridgeport Gas Processing Plant	Bridgeport	Wise	TX	6/9/2008
Houston Central Gas Processing Plant	Sheridan	Colorado	TX	7/7/2008
East Texas Gas Processing Plant	Carthage	Panola	TX	8/25/2008

2.1.9.7 Site Assistance Visit

The Site Assistance Visit (SAV) is an information-gathering visit in which a DHS representative visits an energy-related site to facilitate discussions on identifying and mitigating vulnerabilities between government and industry in the field. It is nonregulatory and is not a vulnerability assessment. Table 2-2 lists energy assets at which SAVs were conducted between May 2007 and May 2008.

Table 2-2: Recipients of SAVs, May 2007–May 2008

Name	City	County	State	SAV Date
ConocoPhillips Wilmington Refinery	Wilmington	Los Angeles	CA	5/14/2007
Sunoco Toledo Refinery	Oregon	Lucas	OH	5/30/2007
Philadelphia Gas Works	Philadelphia	Philadelphia	PA	6/25/2007
Citgo Lemont Refinery	Lemont	Cook	IL	9/18/2007
ConocoPhillips Alliance Refinery–Belle Chasse	Belle Chasse	Plaquemines Parish	LA	10/28/2007
Nelway Substation	Salmo		BC	10/31/2007
Selkirk Substation	Kootenay Boundary		BC	10/31/2007
Bonneville Power Administration (BPA) Boundary Dam Substation	Metaline Falls	Pend Oreille	WA	10/31/2007
Custer Substation	Custer	Whatcom	WA	11/5/2007
Ingledow Substation	Surrey		BC	11/6/2007
William R. Gianelli Pumping-Generating Plant	Gustine	Merced	CA	3/10/2008

Table 2-2 (Cont.)

Name	City	County	State	SAV Date
Pearblossom Pumping Plant	Pearblossom	Los Angeles	CA	4/28/2008
Castaic Powerplant	Castaic	Los Angeles	CA	4/29/2008
Espejo Compressor Station	Rio Rancho	Sandoval	NM	5/11/2008
Public Service Company of New Mexico Gas Electric Dispatch Center	Albuquerque	Bernalillo	NM	5/11/2008
Reeves Generating Station	Albuquerque	Bernalillo	NM	5/11/2008
San Juan Generating Station	Waterflow	San Juan	NM	5/11/2008
West Mesa Switching Station	Albuquerque	Bernalillo	NM	5/11/2008
Devon Bridgeport Gas Processing Plant	Bridgeport	Wise	TX	6/9/2008
Bruce Mansfield Generating Station	Shippingport	Beaver	PA	6/23/2008
East Texas Gas Processing Plant	Carthage	Panola	TX	8/25/2008

2.1.9.8 Comprehensive Reviews

A Comprehensive Review (CR) is a cooperative, government-led analysis of CIKR facilities. Initial efforts have focused on nuclear and liquefied natural gas (LNG) assets. DOE is an active program participant. CRs consider potential terrorist actions that could be involved in an attack; the consequences of such an attack; and the integrated preparedness and response capabilities of the owners and operators, local law enforcement, and emergency response organizations.

2.1.10 Chemical Facility Anti-Terrorism Standards

The Chemical Facility Anti-Terrorism Standards (CFATS), which are implemented by DHS, affect facilities with a specified quantity or more of DHS-defined chemicals of interest (COIs). These standards are likely to affect many facilities in the Energy Sector, specifically the Oil and Natural Gas and Electricity Subsectors, as well as other major sectors of the economy.

The CFATS regulation was published on April 9, 2007, in an Interim Final Rule, codified in Part 27, Title 66 of the *Code of Federal Regulations* (66 CFR Part 27). This regulation requires any facility that possesses any of the COIs that are listed in Appendix A to Part 27 in an amount at or above the applicable screening threshold quantity (STQ) for the chemical to complete and submit an on-line questionnaire (a "Top-Screen") through DHS's Chemical Security Assessment Tool (CSAT).

Once DHS reviews a facility's Top-Screen, it initially either considers the facility to be high risk and places into one of four risk-based tiers or excludes the facility from further regulation under CFATS (barring a change in the facility's operations that would trigger a new Top-Screen). DHS then notifies the facility of its status. Facilities initially determined to be high risk have to complete a security vulnerability assessment (SVA). Certain (Tier 4) facilities are allowed to develop an alternate security program (ASP) in lieu of the CSAT SVA.

After reviewing and approving a facility's SVA or ASP, DHS makes a final determination as to whether the facility is still high risk, and if it is, DHS assigns the facility to a final tier. DHS provides written notification to the facility of its final status after the SVA or ASP review is complete. A facility that is still considered high risk at that point must then prepare a site security plan or an ASP in lieu of the site security plan.

DHS oversees the high-risk facility's development of a site security plan or an ASP to assure that it satisfies the CFATS risk-based performance standards (RBPSs) and that it is tailored to the individual facility's COI and security issues, which could include security measures and policies appropriate to the facility's final tier level and other circumstances.

Initial high-risk determinations, preliminary tiering assignments, and notifications to facilities on whether they are high risk or not were completed for about 32,000 facilities in June 2008. While the number of Energy Sector assets covered by this program is not known at this time, a significant number of both oil and natural gas and electricity assets are expected to be covered.

2.1.11 DOE Fossil Energy Programs

2.1.11.1 Energy Coal and Coal R&D Programs

Energy security goes beyond protecting assets; it involves ensuring uninterrupted energy supplies. As the global demand for energy continues to rise, energy security concerns have become more and more important. The interruption of energy supplies could cause major financial losses. Hence, long-term security and resource availability are also concerns. A diverse mix of energy sources, each with different advantages, provides security to an energy system by giving a country flexibility to meet its energy needs. Coal, as a primary electricity generating fuel in the United States, plays a key role in meeting the Nation's demand for a secure energy supply.

Coal R&D undertaken by DOE's Office of Fossil Energy (FE) is focused on ensuring that indigenous coal resources will continue to be available to enable the country's economic development and to be used to generate needed power, thus serving to guard against import dependence and price shocks. Coal can be stockpiled at mines, power stations, or intermediate locations, and stocks can be drawn on in emergencies.

The development of coal to create liquid fuels could serve to hedge against oil-related energy security risks. By using domestic coal reserves or accessing the relatively stable international coal market, countries can minimize their exposure to oil price volatility while obtaining the liquid fuels needed for economic growth.[11]

[11] For more information, see the World Coal Institute's Web site: http://www.worldcoal.org/pages/content/index.asp?PageID=21.

2.1.11.2 Strategic Petroleum Reserve

The Strategic Petroleum Reserve (SPR) is this Nation's emergency stockpile of petroleum. It was established by Congress to protect the United States against potential disruptions in its critical oil supplies. The SPR has a current inventory of more than 700 million barrels and is worth more than $85 billion. The emergency response mission and the petroleum assets of the SPR make it a CIKR under the NIPP.

The creation of SPR was authorized by the Energy Policy and Conservation Act (EPCA), signed into law on December 22, 1975. EPCA declared it to be the policy of the U.S. Government to maintain a stockpile of crude oil and petroleum products in order to diminish the Nation's vulnerability to the effects of disruptions in petroleum supplies and to meet its obligations under the International Energy Program. EPCA provided the authorization for a reserve of up to 1 billion barrels; however, initial implementation has involved only 750 million barrels.

The SPR Program is managed under the auspices of the Assistant Secretary for Fossil Energy by the Office of Petroleum Reserves. The SPR owns and operates four storage sites — two in Texas and two in Louisiana — with a combined storage capacity of 727 million barrels. The sites are maintained in a posture of high operational readiness; they are capable of responding to an oil supply disruption at a maximum release rate of 4.4 million barrels per day within 15 days after a Presidential Decision.

The SPR uses salt dome storage technology to provide maximum security and safety. Its stockpile of crude oil is stored in large underground storage caverns more than 2,000 feet below the surface. The deep underground caverns have been created in the solid salt formation through solution mining, and they provide pressure-tight spaces that are impermeable to liquids and inert to petroleum. Underground storage assures protection against normal hazards, such as lightning storms and fires, and against the risks of oil leaks and environmental damage. The SPR sites are fully protected by numerous physical security systems to assure protection against any potential terrorism, sabotage, or oil theft. In place at the SPR sites are forces of armed guards with Federal arrest authority, advanced perimeter surveillance and detection systems, restricted vehicle entry policies and vehicle inspection procedures, and controlled personnel access and screening systems.

The SPR has been strategically located in the heart of the U.S. Gulf Coast petroleum refining industry to allow rapid oil distribution via pipelines to the major refining centers, via interstate pipelines to the mid continent, and via marine distribution terminals (figure 2-3). The SPR storage sites have pipeline connections to 49 of the Nation's 149 refineries that import more than 5 million barrels per day. The SPR is also connected to five marine terminals with a combined marine distribution capacity of 2.5 million barrels per day, which provides the capability to supply refineries on the East and West Coasts and in Hawaii, Puerto Rico, and the Virgin Islands.

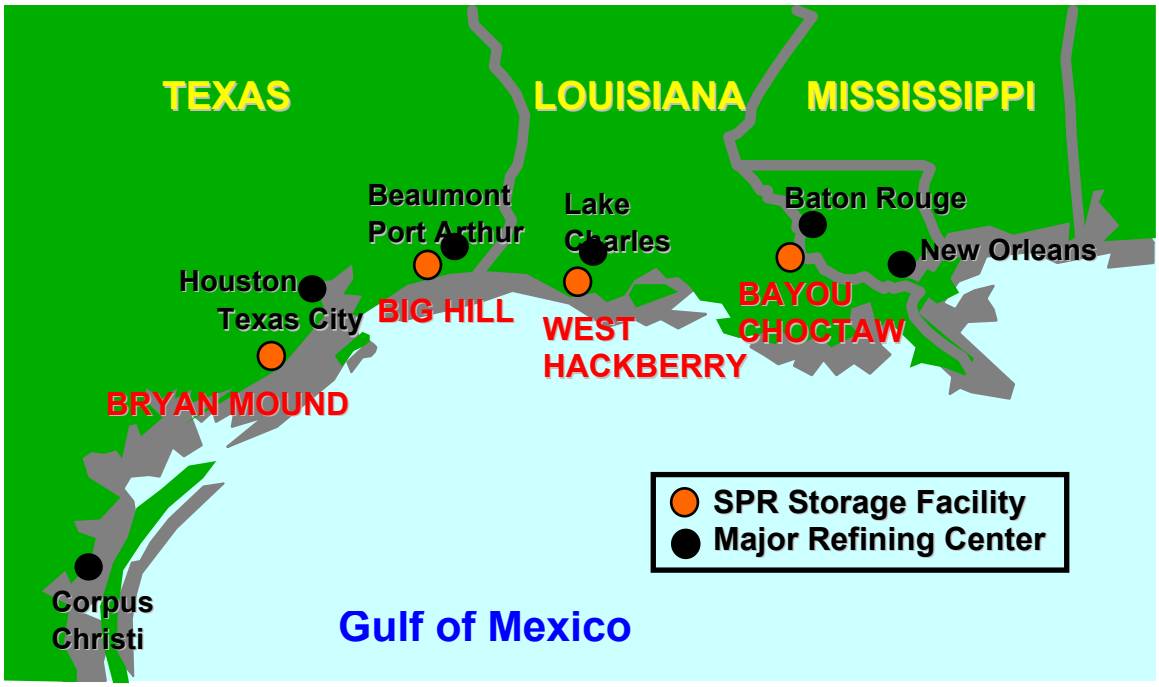


Figure 2-3: SPR Storage Facilities and Major Refining Centers

The current inventory of the SPR is 703 million barrels, which is equivalent to 58 days of net U.S. petroleum imports. The SPR allows the United States to participate in the International Energy Agency (IEA), an international alliance of 26 countries. Each IEA member is required to hold stocks equal to 90 days or more of it net imports (which can also include commercial industry stocks). The IEA maintains agreed-upon mechanisms for coordinating the use of these stocks to respond to a disruption in the global oil supply. The SPR also serves as a national defense reserve, providing a crucial source of petroleum supplies for military needs in the event of a war.

The Energy Policy Act of 2005 directed DOE to acquire petroleum to fill the SPR to a level of 1 billion barrels (section 301) and to complete proceedings to select the sites needed to fill the SPR to this fully authorized volume (section 303). On February 14, 2007, the Secretary of Energy signed a Record of Decision selecting two existing SPR sites for expansion and one new salt dome in Mississippi for the development a new 160 million barrel site to achieve the expansion to 1 billion barrels. This expansion began in 2008 and is expected to attain 1 billion barrels by 2020.

2.1.11.3 LNG Market Trends and DOE-FE Activities

2.1.11.3.1 Growing Role of LNG in the U.S. Gas Market

LNG is quickly becoming an important supply source for meeting U.S. natural gas demand. Net U.S. LNG imports grew from 170 billion cubic feet (Bcf) in 2000 to 720 Bcf in 2007, a fourfold

increase. This development has solidified LNG's role in the U.S. gas market, with LNG making up about 15 percent of U.S. net natural gas imports in 2007 alone.

According to the DOE Energy Information Administration (EIA) publication, *Annual Energy Outlook 2008*, this trend is likely to continue in the future. Recent estimates indicate that LNG imports will grow by an average of 7 percent each year over the next two decades, reaching 2,840 Bcf per day (Bcf/d) by 2030, although much of this growth is likely to take place through 2015. EIA expects this increase to correspond with a significant decrease in natural gas pipeline imports from Canada.

DOE-FE, in addition to tracking commercial LNG activities to support policy decisions, has regulatory authority over the import and export of natural gas, including LNG, to and from the United States. Any party interested in importing or exporting natural gas, including LNG, must first obtain an authorization from DOE. A condition of all authorizations is that each party must report all transactions on a monthly basis. DOE publishes these transactions in monthly and annual reports.

2.1.11.3.2 LNG Infrastructure Locations

Currently, the U.S. has four domestic onshore import terminals, one domestic offshore import terminal, and one onshore export terminal in operation. The five import terminals are located in Everett, Massachusetts; Lake Charles, Louisiana; Elba Island, Georgia; Cove Point, Maryland; and off the Gulf of Mexico. Total nominal regasification capacity for these facilities is 4.471 Bcf/d. The export terminal is located in Kenai, Alaska; it has a nominal liquefaction capacity of 0.186 Bcf/d.

Numerous other import terminals have received commissioning cargoes or been approved for construction. From January to July 2008, three LNG terminals received commissioning cargoes: Freeport LNG in Texas, Sabine Pass in Louisiana, and Northeast Energy Bridge® Gateway in Massachusetts. In addition, Gulf Gateway Energy Bridge® in the Gulf of Mexico is operational and capable of receiving cargo as market forces dictate. Twenty more approved terminals were either not in operation or in the commissioning phase as of April 21, 2008.

2.1.11.3.3 LNG Infrastructure Safety

With LNG gaining prominence as a future U.S. natural gas supply source, DOE has taken steps to improve LNG safety. In December 2004, Sandia National Laboratories published a report entitled *Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill over Water*. The report reviewed several existing studies of LNG spills and provided guidance on the appropriateness of models, assumptions, and risk management efforts designed to address the safety of property and the public with regard to a potential LNG spill over water.

For FY 2008, Congress appropriated $7.9 million for the DOE-FE to conduct studies on two LNG safety topics. The first involves experiments on large-scale LNG pool fires on water to

generate data on fire parameters and provide decisionmakers with relevant information to determine risks from the thermal hazards of LNG fires. The second topic includes a cascading (multitank) failure analysis on an LNG vessel suffering from cryogenic and thermal damage. This study will help determine the possibility of such a failure and the associated consequences on a vessel's structural integrity. The anticipated completion date for this research is December 2009.

2.2 Coordination Groups and Security Partners

Perhaps the most valuable aspect of the Energy SSP development process has been the establishment of open communication and the ongoing development of a trusted relationship between Government and industry — the cornerstone of the overall NIPP strategy. This partnership has enabled the development of a unified set of security goals for the Energy Sector, and it will continue to facilitate the national effort to implement the Energy Sector's CIKR protective programs.

Further, the Energy Sector has established two SCCs and a GCC, in accordance with the CIPAC requirement. The CIPAC, established by DHS to support implementation of the NIPP, activates the sector partnership model set forth in the NIPP. The SCCs and GCC continue to play vital roles in the Energy Sector. Below is a brief update on the security partners' participation; comprehensive information is available in the Energy SSP.

2.2.1 Partnership for Critical Infrastructure Security

The DHS Partnership for Critical Infrastructure Security (PCIS) coordinates cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. This effort spans the full spectrum of critical infrastructure matters, from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery. PCIS focuses primarily on cross-sector policy, strategy, and interdependency issues affecting the critical infrastructure sectors,

The PCIS has enabled critical infrastructure sectors to work among themselves and work in partnership with the Federal Government for the past six years. PCIS was formally recognized as the Private Sector Cross-Sector Council in the NIPP, released in June 2006. Each of the 18 CIKR sectors is represented on the Council.

2.2.2 Electricity SCC

The Electricity SCC represents more than 95 percent of electricity industry owners and operators, including representatives from more than 35 industry companies and organizations. It also includes the executive committee of NERC's CIPC, along with the president and chief executive officer of NERC. The Electricity SCC has continued to meet regularly; it has held

numerous meetings and teleconferences since the submission of the last annual report in July 2007. The organizations currently participating on the Electricity SCC are as follows:

- National Rural Electric Cooperative Association (NRECA).
- Southern Company.
- Arizona Public Service.
- Dominion Resources.
- Hydro One (Ontario, Canada).
- Allegheny Power.
- Arkansas Electric Cooperative Corp.
- North American Electric Reliability Corporation (NERC).
- American Public Power Association (APPA).
- Edison Electric Institute (EEI).
- Independent Electric System Operator (IESO) (Ontario, Canada).

2.2.3 Oil and Natural Gas SCC

The Oil and Natural Gas SCC represents more than 98 percent of oil and natural gas industry owner/operators, with representatives from 22 industry trade organizations. The council chair acts as the primary contact for DHS. The members of the Oil and Natural Gas SCC (table 2-3) also work on Transportation Sector pipeline efforts. In addition to participating in the quarterly CIPAC meetings, the Oil and Natural Gas SCC has held dozens of meetings and teleconferences through its working groups since the submission of the last annual report in July 2007.

Table 2-3: Oil and Natural Gas SCC Members

American Exploration and Production Council	Interstate Natural Gas Association of America
American Gas Association	Independent Petroleum Association of America
American Petroleum Institute	Leffler Energy
American Public Gas Association	Marathon Petroleum Company, LLC
Anadarko Canada Corp.	National Association of Convenience Stores
Anadarko Petroleum Corporation	National Ocean Industries Association
Association of Oil Pipe Lines	National Petrochemical & Refiners Association
BP	National Propane Gas Association
Canadian Association of Petroleum Producers	NiSource, Inc.
Canadian Energy Pipeline Association	Offshore Marine Service Association
Chevron Corporation	Offshore Operators Committee
ConocoPhillips	Petroleum Marketers Association of America
Dominion Resources Inc.	Rowan Companies, Inc.
Edison Chouest Offshore, LLC	Shell Oil Company
El Paso Corp.	Shipley Stores, LLC
ExxonMobil	Society of Independent Gas Marketers Association
Gas Processors Association	U.S. Oil & Gas Association
Independent Liquid Terminals Association	Valero Energy Corporation
International Association of Drilling Contractors	Western States Petroleum Association

2.2.4 Energy GCC

Chaired by DOE, the GCC is the Federal Government counterpart of the sector SCCs. The Energy GCC is composed of representatives across various levels of government (Federal, State, local, tribal, and Territorial) that are concerned with the security of the Energy Sector. Tribal groups are represented on the Energy GCC by the National Indian Health Board. The members of the Energy GCC also work on Transportation Systems Sector pipeline efforts. The Energy GCC plans to meet at least quarterly, and it has held meetings and teleconferences since the submission of the last annual report in July 2007.

The Energy GCC — assisted by joint working groups, the National Association of Regulatory Utility Commissioners (NARUC), and the National Association of State Energy Officials (NASEO) — undertook a significant effort to review and offer extensive comments and suggestions on the Energy SSP during its development in the summer and fall of 2006.

As per a revised Energy GCC charter adopted in May 2008, the objectives of the Energy GCC include the following:

- Provide effective coordination of the many Energy Sector efforts underway to ensure a reliable, secure, and resilient energy infrastructure, including policy and communication across the government and between the government and the Energy Sector to support the Nation's homeland security mission in accordance with NIPP.

- Act as the counterpart and governmental sector partner to the industry-led Electricity SCC and the Oil and Natural Gas SCC, by planning, implementing, and executing sufficient and necessary Energy Sector-wide security programs for the Nation's CIKR.

- Play a coordination role in preparing for and responding to issues that would result from a terrorist act or man-made or natural disaster of national significance that would impact the Energy Sector.

- Act as an advisory, consensus-building group without encroaching upon or abrogating the legal or regulatory responsibilities of the participants.

The Energy GCC will accomplish its objectives through a number of different activities, including the following:

- Identify issues that need agency-to-agency and public-to-private coordination and communication to advance CIP.

- Identify and propose collaborative strategies to correct or eliminate needs, gaps, overlaps, and conflicts in plans, programs, policies, and procedures in order to more efficiently use government resources and reduce any unnecessary burden on the Energy Sector.

- Acknowledge and recognize successful programs and practices.

- Leverage complementary resources within the government and between government and industry.

Participants in the Energy GCC include the following:

- U.S. Department of Energy (DOE).
- U.S. Department of Homeland Security (DHS).
- Transportation Security Administration (TSA), Pipeline Security Division.
- U.S. Coast Guard (USCG).
- U.S. Department of Transportation (DOT), Pipeline and Hazardous Materials Safety Administration (PHMSA).
- U.S. Department of the Interior (DOI), Minerals Management Service (MMS).
- U.S. Department of Agriculture (USDA), Rural Utility Services (RUS).
- U.S. Department of Defense (DoD).
- Federal Energy Regulatory Commission (FERC).
- U.S. Environmental Protection Agency (EPA).
- National Association of Regulatory Utility Commissioners (NARUC).
- National Association of State Energy Officials (NASEO).
- National Governors Association (NGA).
- Canadian Department of Natural Resources (NRCAN).
- U.S. Department of the Treasury.

The Energy GCC may also ask other departments and agencies to participate in Energy GCC activities on an ad-hoc basis.

The Energy GCC seeks to develop a consensus on issues and recommendations without voting. Council members work through a consultative process, encouraging the exchange of information and points of view, thus striving for consensus.

2.2.5 State, Local, Tribal, and Territorial (SLTT) GCC

The SLTT GCC is a newly formed council that consists of State, local, tribal, and Territorial government security partners who are critical in NIPP implementation. The SLTT GCC consists of security partners from all CIKR sectors. Two representatives with energy backgrounds have been appointed to work with the Energy GCC.

Prior to the formation of the SLTT GCC, DOE had established liaisons with State, local, tribal, and Territorial government agencies responsible for preventing and responding to energy disruptions. These entities are responsible for conducting emergency planning and response, developing energy security and reliability policies and practices, and facilitating Energy Sector protection activities. Therefore, they play a significant role in preventing energy supply crises and mitigating emergency impacts that could arise. DOE will continue to strengthen these relationships through the newly formed SLTT GCC and other specific initiatives.

State, local, tribal, and Territorial governments play an important role in securing the Nation's energy infrastructure. DOE-OE has been working closely with these governments to ensure a coordinated effort at the Federal, State, local, tribal, and Territorial levels. The NGA's Center for Best Practices, NARUC, NASEO, the National Conference of State Legislatures (NCSL), and Public Technologies Institute (PTI) are partners that have been working jointly in this effort. Examples of State and local government programs and initiatives that directly support NIPP implementation are included in attachment D: Draft — State and Local Initiatives for the 2008 Sector CIKR Protection Annual Report for the Energy Sector.

More specific examples of programs and initiatives undertaken by the State and local government groups that directly support NIPP implementation are included in attachment G, Energy Sector Protective Programs. This attachment summarizes additional activities undertaken by the various groups since the 2007 annual report was submitted.

2.2.6 Other State, Local, Tribal, and Territorial Activities

State, local, tribal, and Territorial governments play an important role in securing the Nation's energy infrastructure. Efforts to implement the Energy SSP at the State and local levels are supported and coordinated by NASEO, NARUC, the NGA Center for Best Practices, NCSL, and PTI. These groups have undertaken significant efforts to work toward the goals and objectives of the Energy SSP and have diligently sought to ensure that critical energy infrastructures are appropriately protected, investments are made to enhance resiliency, and State and local governments are prepared to quickly and effectively respond in order to support and complement the private sector's response to energy disruptions. Both NASEO and NARUC representatives have participated in the GCC meetings and briefed other State and local partners on these meetings.

Some key State-level and local-level activities that these groups have engaged in to achieve better preparedness and enhanced energy infrastructure resiliency are as follows:

- *Security partner planning meeting.* The meeting, involving State and local participating organizations, was held by DOE-OE on August 7, 2007, in Hershey, Pennsylvania. In addition to reviewing progress during the past year, attendees discussed FY 2008 priorities and explored program concepts for the coming years. Participants identified common areas of interest and potential points of collaboration; this effort has helped guide the work of these groups over the last year.

- *Black Water–Southeast Energy water interdependence exercise.* NASEO and NARUC staff supported DOE-OE in planning and coordinating the tabletop exercise held April 24 and 25, 2007, in Decatur, Georgia. The objective of the exercise was to increase participant understanding of the interdependencies between the Energy Sector and the water supply and wastewater management system.

- *Dark Storm: Northeast energy assurance exercise.* NASEO and NARUC staff members were responsible for the logistical planning and coordinating of this exercise held June 19

and 20, 2007, in Princeton, New Jersey. NCSL, NGA, and PIT also supported this effort. The exercise attracted more than 90 participants from 11 State and Territory energy offices in the Northeast and Mid-Atlantic Regions.

- *Workshop on building resiliency into energy assurance planning.* This workshop, held on April 22 and 23, 2008, in Denver, Colorado, was organized in conjunction with DOE's Summer Fuels Outlook Conference. It was sponsored by DOE, NCSL, and the Pacific Northwest Economic Region (PNWER), with support from NARUC, NASEO, NGA, and PTI, all of whom participated. The workshop was attended by representatives from the Federal and State governments, select private sector participants, nonprofit organizations, and major municipalities and local governments. State agencies included public utility commissions, energy offices, emergency management agencies, homeland security advisors, and administrators.

Examples of State, local, and Territorial government programs and initiatives that directly support NIPP implementation are included in attachment D, "State, Local, and Territorial Initiatives for the 2008 Sector CIKR Protection Annual Report for the Energy Sector."

2.2.7 Working Groups

In addition to the Energy Sector GCC and SCCs, several working groups have been established and are currently in operation. They are described briefly in the following sections.

2.2.7.1 Joint Energy Metrics Working Group

2.2.7.1.1 CIPAC Metrics Working Group

The Joint Energy Working Group established a subgroup, the Metrics Working Group, to address the important subject of metrics. While there is a single group consisting of Energy GCC, Oil and Natural Gas SCC, and Electricity SCC members, each subgroup differs in its approach to metrics development. DOE and its Energy Sector security partners need to consider the sensitivity of some data as well as the need to protect information from unintended disclosure or inappropriate use. Energy Sector asset owners and operators have focused on metrics for their internal use, but the subject of CIP metrics for subsectors requires further discussion with regard to who will collect the data and they will do it. DOE is working with other federal agencies, including those in the Water Sector and Healthcare and Public Health Sector, who are also addressing these issues.

Metrics Working Group members include several members of the NERC CIP Executive Committee, DoD, DHS (including IP and TSA), AGA, NPRA, API, NiSource Inc., Questar Gas Company, NERC, FERC, Chouest-Edison Energy, NRECA, DOI (MMS), NARUC/NASEO, and Energetics, Inc.

2.2.7.1.2 Electricity Subsector

Since NERC was established as the ERO under the Energy Policy Act of 2005, nearly 100 reliability standards are currently enforceable, including those related to both physical and cyber security. Because the standards that focus on cyber security are implemented by utilities, the results will need to be reported to NERC and FERC. These standards are now in various stages of implementation; reporting will begin in 2009 and continue beyond. DOE, in cooperation with NERC and FERC, will develop metrics that will track industry performance and be appropriate for reporting progress.

2.2.7.1.3 Oil and Natural Gas Subsector

As an active participant in the Metrics Working Group, DOE has begun discussions with Energy Sector partners (in both the Electricity and the Oil and Natural Gas Subsectors) on the metrics that could be used. It has provided a list of potential metrics in 18 categories, as follows:

1. Restricted area perimeter.
2. Securing of site assets.
3. Screening and access controls.
4. Deterrence, detection, and delay.
5. Shipping, receipt, and storage.
6. Theft and diversion.
7. Sabotage.
8. Cyber issues.
9. Response.
10. Monitoring.
11. Training.
12. Personnel surety.
13. Elevated threats.
14. Specific threats, vulnerabilities, or risks.
15. Reporting of significant security incidents.
16. Significant security incidents and suspicious activities.
17. Officials and organizations.
18. Records.

Discussions with industry representatives will help to determine a select number of metrics that will be appropriate. Regulatory programs administered by DHS and other groups (including State and local governments) also require reports from which measures of industry performance may be examined.

2.2.7.2 Energy Sector Control Systems Working Group

The Energy Sector Control Systems Working Group was established as a joint group under CIPAC.[12]

2.2.7.3 Oil and Natural Gas SCC Emergency Management Working Group

The terrorist attacks of 9/11, coupled with the 2005 Gulf Coast hurricanes, have led to many national plans and strategies that have greatly increased the need for a better understanding of the disciplines involved in emergency management (EM). EM is part of maintaining business continuity (i.e., continuity of operations). Business continuity involves preparedness, prevention, response, recovery, and mitigation. EM focuses on preparedness, response, recovery, and mitigation, with prevention usually being integrated into facility operations and maintenance. DHS plans and strategies include the NRF, National Incident Management System (NIMS) policy, NIPP, and the DOE ESSP.

Like their government counterparts, the private sector has focused on response and recovery capabilities. Since its formation in 2004, the industry Oil and Natural Gas SCC has provided an excellent opportunity for representatives of both the private and public sectors to discuss and exchange information to help protect the Nation's oil and natural gas and chemical CIKR. This SCC, which is composed of Oil and Natural Gas Subsector owners and operators (representing more than 98% of the industry), provides a central forum for exchanging information, resolving issues, and introducing value-added solutions and initiatives. To ensure the strength of the oil and natural gas and chemical industries' EM capabilities, the Oil and Natural Gas SCC established a collaborative Emergency Management Working Group (EMWG) with the Chemical SCC. This council supports the EM capabilities of these two industries by facilitating discussions and sharing of EM information.

Objectives of the EMWG include but are not limited to the following:

- Increase communication and coordination with DOE, DHS, and other agencies in the Energy GCC and Chemical GCC on managing incidents and emergencies.
- Promote EM as it relates to IP and serve as a focal point on EM for national plans and programs (e.g., NIMS, National Contingency Plan (NCP), NIPP, ESSP, Homeland Security Exercise and Evaluation Program).
- Provide a forum for industry and government agencies to share information on Federal regulations and programs that may affect EM activities and programs in the Oil and Natural Gas Subsector and Chemical Sector.

[12] See discussion in section 3.

- Facilitate informative dialogs between oil and natural gas industry members to help individual companies develop and periodically assess EM.
- Discuss EM practices and lessons learned.
- Serve as a liaison between the industry and government on R&D that would enhance the Nation's emergency preparedness and response capabilities.

The EMWG reports to the Oil and Natural Gas SCC Chair and to the Chemical SCC and meets at least twice a year.

2.2.7.4 Pipeline Working Group

The Oil and Natural Gas SCC established a Pipeline Working Group that works closely with TSA and PHMSA on pipeline security issues.

2.2.8 Cooperation with Other Agencies

DOE works closely with several other federal agencies, including the U.S. Department of Health and Human Services (HHS) on pandemic-related issues and DOT on providing support on outages and restoration during energy emergencies.

2.2.8.1 Department of Health and Human Services

DOE participated in a high-level HHS exercise with the HHS Secretary's operation center that involved energy-related impacts. DOE and HHS conducted a joint exercise to explore closer cooperation.

2.2.8.2 Banking and Finance

The Energy Sector is also collaborating with the Banking and Finance Sector. For example, the Visualization and Modeling Working Group (VMWG)[13] provides the Banking and Finance SCC with information about hurricanes and the power outages that might result from them. This information allows financial institutions in the affected areas to better prepare for and recover from these storms. Moreover, in addition to maintaining individual relationships with utilities, some regional coalitions of financial institutions within the Banking and Finance Sector have made arrangements with local utilities to serve as information conduits in the event of a widespread outage.

13 See attachment E for more information on the VMWG.

2.2.8.3 Other Agencies

DOE, through the VMWG, also cooperates with the U.S. Army Corps of Engineers (USACE) and other agencies on an ongoing basis. The USACE has become a core member of DOE modeling and analysis efforts.

Section 3: CIKR R&D Progress and Updated Capability Gaps

The Energy Sector envisions a "robust and resilient energy infrastructure." This cannot be achieved without continuous and significant capital investment in new R&D efforts of both the private and public sectors. Energy Sector security partners have become increasingly concerned about the security of the energy infrastructure in today's rapidly changing world. Since the 1990s, various groups have conducted numerous studies on the vulnerability and reliability of the energy infrastructure and have examined R&D needs in a new threat environment. Currently, industry and government are actively working together to coordinate technology development through R&D roadmaps, government program reviews, and professional conferences and workshops to leverage limited resources for maximum gain. Chapter 7 of the Energy SSP provides a thorough review of the Energy Sector R&D planning requirements.

3.1 Progress

DOE-OE has been working with the private sector to enhance CIP since the 1990s, as described in the following sections.

3.1.1 Roadmap to Secure Control Systems in the Energy Sector

In 2003, DOE, working in partnership with the oil, gas, and electricity industries, began developing its Roadmap. Although a number of activities designed to help secure control systems were underway at that time, there was no clear vision or strategic framework for coordinating these diverse activities. The private sector — which collectively owns and operates about 80 percent of U.S. Energy Sector assets — also lacked a compelling business case to support investment in cyber security. Coupled with the scope and complexity of the problem, these issues underscored a significant need for increased public–private partnerships to maximize limited resources and effectively enhance control system security. The Roadmap addressed these needs by establishing a vision and laying out a coherent plan for cyber security in the Energy Sector.

The Roadmap envisions that "in 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function." To achieve this vision, the Roadmap established a framework that is based on sound risk management principles and features the following four strategic goals:

1. *Measure and assess security posture.* Within 10 years, the Energy Sector will help ensure that energy asset owners have the ability and commitment to perform fully automated monitoring of their control system networks' security with real-time remediation.

2. *Develop and integrate protective measures.* Within 10 years, next-generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.

3. *Detect intrusion and implement response strategies.* Within 10 years, the Energy Sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.

4. *Sustain security improvements*. Over the next 10 years, energy asset owners and operators are committed to working collaboratively with government and sector security partners to accelerate security advances.

To help the industry track its progress in implementing the Roadmap, DOE created ieRoadmap (Interactive Energy Roadmap), a Web-based tool that allows principal investigators to register and self-populate a database that links to the challenges identified in the Roadmap. So far, 96 projects from nearly 20 public and private organizations have been launched supporting the goals identified in the Roadmap. The ieRoadmap (hosted on the Process Control Systems Forum Web site at www.pcsforum.org/roadmap) provides a mechanism to encourage collaboration, identify active areas of work, expose gaps, and enable partners to leverage resources, as well as to inform owners and operators of emerging technologies.

After receiving positive feedback from the Energy Sector on the Roadmap, the NERC CIPC voted unanimously to approve and support the implementation of the Roadmap. In addition, a 2007 report from the U.S. Government Accountability Office, entitled *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are under Way, but Challenges Remain,* commended the Roadmap efforts. The industry experts interviewed to develop the report stated that the Roadmap was a "positive step for the industry" and that the Roadmap process "succeeded in identifying industry needs and was a catalyst for bringing agencies and Government Coordinating Councils together."

The Roadmap has also received recognition from outside the Energy Sector. In a January 16, 2007, report to President Bush, the National Infrastructure Advisory Council (NIAC) recognized the Roadmap's success in developing and implementing cyber security solutions for control systems. The report recommended that all critical infrastructures use the Energy Sector Roadmap as a model to develop their own sector-specific roadmaps.

3.1.2 National SCADA Test Bed Program

DOE supports the Roadmap primarily through its National SCADA Test Bed (NSTB) Program, which conducts cyber security assessments of control systems and related technologies, develops advanced control system technologies, conducts modeling and simulation to better evaluate risk, and engages in industry partnership and outreach.

The program supports the National SCADA Test Bed, a suite of facilities to help the Energy Sector and equipment vendors test control systems to identify potential vulnerabilities. To date, the NSTB has conducted test bed and on-site field vulnerability assessments of 15 control systems from vendors including ABB, Areva, GE, OSI, Siemens, and Telvent. NSTB also conducted assessments of four control system component technologies. As a result of this work, six next-generation "hardened" systems have been developed by the participating vendors, and at

least 21 of one vendor's hardened systems have been deployed in the marketplace. Further, five software patches have been issued by participating vendors that address six critical security issues in response to vulnerabilities discovered by NSTB. One particular software patch issued by a vendor to secure its legacy systems has been downloaded by 82 utilities currently operating those systems. The Council on Competitiveness, in its 2007 report entitled *Transform. Enterprise Resilience: The Resilient Economy; Integrating Competitiveness and Security,* stated that each control system assessed by NSTB "represents a class of more secure SCADA technology, creating a powerful multiplier effect on energy resilience nationwide."

System assessments have revealed common vulnerabilities and easy-to-implement, immediate security fixes that are applicable across the board. Outreach has helped disseminate this knowledge effectively. For example, more than 1,700 Energy Sector security partners have participated in training workshops conducted by NSTB that educate system operators on effective security practices for control system security. In addition, NSTB partners with the NERC Control Systems Security Working Group to publish mitigations for the vulnerabilities identified in the annual report entitled *Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations.*

Recently, DOE also awarded $8 million to five industry projects that are developing and integrating technologically advanced controls and cyber security devices into the Nation's electric grid and energy infrastructure:

1. *Hallmark Project.* This project will commercialize the Secure SCADA Communications Protocol (SSCP). It involves Schweitzer Engineering Laboratories, Pacific Northwest National Laboratories, and CenterPoint Energy.

2. *Detection and Analysis of Threats to the Energy Sector (DATES).* This project will develop an intrusion detection system (at the network, host, and device levels), an event correlation framework, and a Sector-wide, distributed, privacy-preserving repository of security events to which participants can automatically contribute without attribution. It involves SRI International, ArcSight, Sandia National Laboratories, and the Electric Reliability Council of Texas (ERCOT).

3. *Cyber Audit and Attack Detection Toolkit.* This project will extend the capability of existing vulnerability scanning tools to evaluate SCADA security configurations (supporting compliance with NERC CIP-005 and CIP-007) and develop templates for a security event monitoring system. It involves Digital Bond, Tenable Network Security, OSIsoft, Constellation Energy, PacifiCorp, and the TVA.

4. *Lemnos Interoperable Security Program.* This project will conduct testing, validation, and outreach to increase the availability of cost-effective, interoperable security solutions for Internet Protocol-based communications. It involves EnerNex Corp., Schweitzer Engineering Laboratories, the TVA, and Sandia National Laboratories.

5. *Protecting Intelligent Distributed Power Grids against Cyber Attacks*. This project is developing a risk-based critical asset identification system and an integrated and distributed security system with optimization to establish the best topology for networking the security components. It involves Siemens Corporate Research, Idaho National Laboratory, and Rutgers Center for Advanced Energy Systems.

For descriptions of additional public- and private-sector projects addressing Roadmap challenges and goals, visit the ieRoadmap at www.pcsforum.org/roadmap.[14]

3.1.3 Energy Sector Control Systems Working Group

Energy industry leaders formed the Energy Sector Control Systems Working Group for the express purpose of guiding the implementation of the Roadmap. The working group, which ratified its charter in December 2007, is made up of representatives from the Energy GCC, Electricity SCC, and Oil and Natural Gas SCC. It operates under the framework of CIPAC, a group formed under NIPP to support private sector and government collaborations on CIP activities. Working group members have outlined four objectives for their efforts:

- Help identify and implement practical, near-term activities that are high priority for the industry.
- Promote the value of achieving the goals of the Roadmap to the industry.
- Recommend critical areas for public and private investment.
- Measure progress achieved toward meeting Roadmap goals and milestones.

The working group held its first ieRoadmap Workshop in Chicago on May 28 and 29, 2008, to review ongoing R&D projects. The project leads presented their control system security R&D projects to the working group and other security partners and received valuable feedback on how their project aligns with Roadmap goals and how they might improve the relevancy of their project results.

Working group members include Alliant Energy, Alyeska Pipeline, BP, CenterPoint Energy Inc., DHS National Cyber Security Division (NCSD), DHS Directorate of Science and Technology (S&T Directorate), DOE, El Paso Corporation, Entergy Corporation, Ergon Refining Inc., IESO Ontario, and NiSource.

---

[14] For more information, see the following:

- DOE NSTB Program (www.oe.energy.gov/controlsecurity.htm).
- Argonne National Laboratory (www.iac.anl.gov).
- Idaho National Laboratory (www.inl.gov/scada).
- Oak Ridge National Laboratory (http://www.ioc.ornl.gov/welcome.shtml).
- Pacific Northwest National Laboratory (homeland-security.pnl.gov/cip.stm).
- Sandia National Laboratories (www.sandia.gov/scada).
- DHS NCSD (http://www.dhs.gov/xabout/structure/editorial_0839.shtm).
- Process Control Systems Forum (www.pcsforum.org).
- US-CERT (www.us-cert.gov).

3.2 Capability Gaps

The problem of securing the Nation's energy infrastructure is vast in both scope and complexity. Some of the biggest challenges to achieving the vision outlined in the Sector Roadmap include these:

- *Keeping pace with the rapidly changing and growing threat environment.* New cyber vulnerabilities are discovered on a weekly basis. Sophisticated software tools, widely available on the Internet and sometimes traded for profit by cyber extortionists, allow hostile actors to develop and launch new cyber attacks faster than ever (even with limited control system knowledge). The result is a vicious cycle in which there is a constant need for new countermeasures that require increasingly faster implementation.

- *Accelerating the commercialization of inherently secure and resilient control systems.* As these systems become more integrated into enterprise and corporatewide systems, it is essential to transform the state of the art of control system technology from an inherently insecure technology that requires layers of defense and costly management processes to a technology that provides built-in security and robustness.

- *Increasing understanding of cyber risks.* While our understanding of the risk of cyber attacks on the energy infrastructure has been improved through Roadmap-related R&D, energy asset owners and operators still do not have the capabilities to fully understand the risks associated with the cyber threats of today and tomorrow. Without a better understanding of these risks, costs, and potential consequences, it will continue to be difficult to make a strong business case for cyber security investments.

Table 3-1 lists R&D capability requirements for the Energy Sector.

Table 3-1: Research and Development Capability Gaps

Question	Response
Capability gap statement tracking and priority number	2008–001–Energy
Proposed title of requirement	Recovery Transformer
Goal/objective to which requirement responds	Energy SSP Physical and Cyber Security Goal 2: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.
Theme	Advanced infrastructure architectures
Threat identification	The threat is failure of a high-voltage transformer; a new transformer can take 2 to 3 months to install and has a long manufacturing lead time (often more than 18 months), and there is limited/no domestic manufacturing capability.

Table 3-1 (Cont.)

Question	Response
Gaps of existing capabilities	There is a need for a new type of emergency spare (recovery/mobile) high-voltage transformer that can be deployed and energized quickly to rapidly recover from outages caused by natural disasters and deliberate attacks.
Description of required operational capability	The recovery transformer must be able to be deployed and installed within days (e.g., two days to deliver and two days to energize), not months. Size/rating should be adaptable/modular to flexibly accommodate the needs of the utility industry.
Identification of existing related capabilities or technology	Previous research and analysis by DOE in high-temperature superconductivity, solid-state materials (power electronics), electrical steel, core design, and mobile transformers/substations could be leveraged to meet project objectives.
Identification of possible approaches/solutions	R&D, testing, and field demonstration of a single-phase high-voltage unit, at a minimum.
Capability gap statement tracking and priority number	2008–002–Energy
Proposed title of requirement	Cyber Security for Control Systems
Goal/objective to which requirement responds	Energy SSP Physical and Cyber Security Goal 2: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.
Theme	Protection and prevention systems
Threat identification	Energy Sector control systems were originally designed for reliability, with little attention given to cyber security. Cyber threats are escalating, and the knowledge required to launch sophisticated attacks is decreasing.
Gaps of existing capabilities	The *Roadmap to Secure Control Systems in the Energy Sector* (January 2006) identifies the gaps in existing capabilities.
Description of required operational capability	The capabilities of the threat continue to evolve and adapt as new defenses are developed and deployed. Next-generation control systems are needed that can survive an intentional cyber assault with no loss of critical functions. Required operational capabilities include: ▪ Fully automated security state monitoring with real-time remediation. ▪ Components and architectures with built-in, end-to-end security. ▪ Automatic contingency and remedial actions in response to attempted intrusions.
Identification of existing related capabilities or technology	Previous R&D by the DOE NSTB Program in vulnerability assessments, advanced technologies, and risk analysis could be leveraged to meet the objectives.
Identification of possible approaches/solutions	R&D, testing, and field demonstration of control systems with cost-effective, hardened operating systems and secure, self-healing architectures that do not adversely affect the overall system reliability, availability, and safety.

Section 4: Funding Priorities

4.1 Planned SSA Investments

DOE-OE and ISER budgets have supported responsibilities associated with DOE's designation as the Energy SSA. Since DHS's approval of the Energy SSP, DOE has been working closely with the Office of Management and Budget (OMB) and other Energy Sector security partners to determine program priorities and requirements identified in the Energy SSP, including human, cyber, and physical security elements.

In addition, OE conducts a diversified reliability-related R&D program focused on the electricity grid, portions of which include visualization and controls, as well as distributed energy resources that support hardening of the electrical system. The Administration has strongly supported this program in its budgets submitted to the U.S. Congress. The funds available for this work are determined by Congress through its annual appropriation process. Table 4-1 presents information on the Sector's annual budget reporting.

Table 4-1: Energy SSA Funding Items

Sector:	Energy							
Agency:	U.S. Department of Energy; Office of Electricity Delivery and Energy Reliability							
					Budget			
Program/ Investment Title	Priorities Addressed	Description of How Program/ Investment Supports CIKR Protection	Office of Management and Budget Account	Included in the HSDB?	FY 2008 Request ($ in thousands)	FY 2008 Enacted ($ in thousands)	FY 2009 Request ($ in thousands) (est.)	FY 2009 Enacted (est.)
Operations and Analysis/ Infrastructure Security and Energy Reliability		Supports DOE ESF-12 support activities; modeling, visualization, and analysis of energy-related events; and cooperation with Energy Sector partners	TD.54.00.00.0/ TD.50.02.00.0		5,860	5,807	7,622	N/A
Renewable and Distributed Systems Integration (formerly Distributed Systems Integration)		R&D on various distributed energy technologies in order to help improve redundancy and resiliency in the electricity system	TD.50.09.00.0		25,700	24,753	33,306	N/A
Visualization and Controls		R&D on advanced control systems, including SCADA systems, in order to improve system reliability and reduce the impacts of possible energy-related events	TD.50.08.00.0		25,305	24,373	25,305	N/A

4.2 Non-SSA Investments

Outside the SSA investments, no detailed spending profile for the Energy Sector is currently available. Besides, the magnitude of spending may not be the best measure of Sector efforts or performance. As stated in chapter 7 of the Energy SSP, R&D is a key source of innovation and enhanced productivity for the Energy Sector. Much of the investment in new technologies and in improving current technologies is undertaken by the suppliers in the electricity and oil and natural gas industry, not the companies themselves. Building a business case for sector investments is a high priority for a sector in which resources are targeted to the best return on investment.

Energy asset owners and operators have worked with government, national laboratories, universities, industry organizations, and other key security partners to drive technological innovation throughout the Energy Sector. Over the past several years, vying for energy supplies has intensified globally, with rapid economic growth in several developing countries. The need for incremental energy supplies and additional energy infrastructure has significantly increased, and it is therefore believed that industry investment in R&D has also increased.

Billions of dollars have been and are being spent by the electric power industry and the oil and natural gas industry to improve the reliability, survivability, and resiliency of their assets. Other sectors have become increasingly aware of their dependence on electricity and seem to be focusing on backup power options. Limited information is available on steps taken, but both the Water and Healthcare and Public Health sectors are seeking to better understand available backup power for their assets.

4.3 Gaps

The Energy Sector is being increasingly recognized by other CIKR sectors as being critical to their operations. A better understanding of the interdependencies among other CIKR sectors, such as Transportation Systems, Banking and Finance, and Communications, is needed to develop approaches and systems to better protect, mitigate, and restore these critical systems after energy-related emergencies. Working closely with Energy Sector security partners, DOE continues to address needs in this area, including physical assessments and self assessments, cyber security, dependency analysis, outreach and education, communications, and information sharing. Considerable efforts are already under way or are planned by Sector security partners, and no major new efforts are foreseen at this time.

Further, the threats of international terrorism, combined with increasing energy consumption in developing nations, continue to pressure energy prices worldwide. DOE is aware of such vulnerabilities and has begun to work with foreign governments in cooperation with the U.S. Department of State to improve energy security through CIP beyond national borders.

Funding priorities for Energy SSP-related activities are discussed in chapter 8 of the Energy SSP, and no significant changes in these priorities are foreseen at this time. The Energy SSP development process and R&D Roadmap have continued to help identify gaps in current programs and approaches. Continued R&D funding support and progress will be critical to the Energy Sector.

This page intentionally blank

Section 5: CIKR Protection: Security Practices and Obstacles

5.1 CIKR Protection Security Practices

As demonstrated in the Energy SSP, both the Electricity Subsector and the Oil and Natural Gas Subsector have taken several voluntary and proactive measures to address increasing concerns about their CIKR protection security. The following subsections highlight some of the ongoing and established security practices in these Subsectors, as well as some of DOE's key initiatives for the Energy Sector as a whole.

5.1.1 Oil and Natural Gas Subsector Security Practices

The Oil and Natural Gas Subsector has proactively implemented various security practices, including developing security standards and guidelines and holding discussions through security committees. Some of the security guidelines and standards that this Subsector currently follows are listed here:

- Security Guidelines: Natural Gas Industry, Transmission and Distribution (AGA/INGAA/American Public Gas Association [APGA]).
- Cryptographic Protection of Supervisory Control and Data Acquisition (SCADA) Communication (AGA Report No. 12-1).
- Security Guidelines for the Petroleum Industry (API).
- Security Vulnerability Assessment Methodology (API/NPRA).
- Pipeline SCADA Security Standards (API Standard 1164).

These guidelines provide an approach for vulnerability assessments, critical facility definition, detection and deterrent methods, response and recovery guidance, cyber security information, and relevant operational standards.

The industry security guidelines incorporate a risk-based approach for natural gas companies to consider when identifying critical facilities and determining appropriate actions. These guidelines are developed on the basis of the DHS Homeland Security Advisory System. The TSA, along with the PHMSA, is currently conducting on-site reviews on the basis of these guidelines.

5.1.2 NERC Electric Reliability Organization and Electric Security Standards

Like the Oil and Natural Gas Subsector, the Electricity Subsector has active security committees and has been proactive in developing industry security guidelines. One of the most notable efforts with regard to cyber security in this subsector has been the establishment of the ERO and the development of mandatory reliability standards. On July 20, 2006, FERC certified NERC as the ERO for developing and enforcing mandatory reliability standards for the bulk power system. Acting under the oversight of FERC, the ERO can impose penalties on a user, owner, or operator of the bulk power system for violations of any FERC-approved reliability standard. Such penalties are subject to FERC review and potential change. Further, FERC has approved the establishment of eight regional entities to receive limited authority from the ERO to develop and regionally enforce mandatory reliability standards that have been approved by FERC.

On March 16, 2007, FERC issued an order approving and establishing the first set of 83 mandatory and enforceable reliability standards; 24 additional proposed standards are pending approval. In addition, on January 18, 2008, FERC approved reliability standards addressing CIP that were proposed by NERC. These reliability standards address the electronic and physical protection of cyber assets that are critical to the operation of the bulk power system. As directed by FERC, NERC is currently modifying these reliability standards to address specific concerns. The ERO has made several other filings with FERC seeking approval for small groups of new reliability standards, including proposed standards that address facility design, connections, maintenance, and transfer capabilities, and regional standards for the Western Electricity Coordinating Council. There are currently about 100 mandatory reliability standards in place.

All of the NERC reliability standards are measurable and satisfy one or more of the Energy Sector security goal categories (see section 1.1). Attachment H: NERC Reliability Standards — Status and Sector Goal Category identifies these reliability standards, the security goal category they relate to, and their current status.

5.1.3 Energy Sector Initiatives

A number of ongoing initiatives in the Energy Sector have been identified as being particularly effective, including the following:

- DOE has integrated HSPD-7 and HSPD-8 activities into a single organization that has enabled faster communication and actions and has helped build the partnership with Energy Sector security partners. This effort has supported the integration and review of the NRF, NIPP, and ESSP.

- DOE's cyber security R&D Roadmap efforts have won wide recognition and support from Energy Sector security partners as well as from President Bush's National Infrastructure Advisory Council (NIAC). In fact, NIAC recommended that all critical infrastructures use the Roadmap as a model to develop their own sector-specific roadmaps.

- The Energy Sector's pandemic planning and its participation in developing policies to support CIP have been models for other sectors.

- Energy Sector training activities to support the Sector's resiliency, reliability, and survivability are well developed and are followed (see attachment F).

- DOE issued a redacted version of the Energy SSP that has received wide distribution among Energy Sector security partners, promoting partnership and cooperation.

- DOE has developed an ISERnet Web site to share information with State and local officials and to support Emergency Support Function 12.

In addition, a large number of the activities listed in attachment G: Energy Sector Protective Programs have received wide support and praise from Energy Sector security partners and have been widely distributed and used.

5.2 Obstacles

While DOE, in partnership with other government agencies and industry, has taken significant strides toward securing CIKR in the Energy Sector, an analysis of metrics data shows several gaps and challenges to achieving this mission that continue. These including the following:

- Data collection is costly and time consuming.

- Energy Sector security partners participate on a voluntary basis, and there are limits on their available time. Creative approaches are needed to encourage and ensure participation over time.

- Some of the data that could be collected are sensitive. Some partners are unwilling or unable to provide certain types of information. Despite challenges, Energy Sector security partners are working to continuously implement improved principles and approaches in order to address the challenges identified in the Energy SSP.

- Information marking and protection approaches need development and acceptance by Energy Sector partners.

- Interdependencies need to be identified so effective outreach can be conducted throughout the supply chain and with other sectors that depend on energy.

- There is a need for cyber security strategies and processes at the national level to allow better integration between sectors.

- The value of the NIPP public/private partnerships and the CIPAC mechanism must be communicated to CIKR owners and operators.

- Communication mechanisms need to be developed to increase the timeliness and availability of key information.

Protecting and improving the resiliency of the Energy Sector are thus ongoing efforts, in which the collection and examination of data on the sector-specific and core metrics will be done continually to identify any gaps and thereby guide further actions to enhance the security of the Sector's infrastructure.

Section 6: Program Effectiveness and Continuous Improvement

In the past year, DOE and Energy Sector activities continued to strengthen the value-added proposition of the NIPP partnership model, helping to achieve the Sector's security goals as outlined in the Energy SSP. Forging a partnership between government sectors and the energy industry underlies the Energy Sector's strategy for implementing the NIPP risk management framework. The Sector's goals have helped focus industry efforts in making risk management decisions and investments, and its partnership strategy has been a key factor in guiding the Sector's risk-reduction activities.

As the Energy SSA, DOE has worked with HITRAC to identify threats and focus analysis efforts on important Sector assets, networks, and functions (Tier 1 and Tier 2). DOE has aligned its sector protection and risk management programs with the risk profiles developed by industry or those based on HITRAC, law enforcement, or other intelligence sources.

The following sections provide a summary of the overall progress of the Energy Sector's CIKR protection efforts and outline the next steps in achieving the goals and objectives set forth in the Energy SSP.

6.1 CIKR Protection Mission Progress

The progress of the Energy Sector's CIKR protection efforts is based on an analysis of metrics that were developed to support the Sector's CIKR protection mission requests. These metrics, based on the implementation actions specified in the NIPP, Energy SSP, and Energy Sector Annual Report, provide a high-level description of Sector activities, projects, and tools and their contributions to the Sector security goals. The Energy Sector's responses to the set of metrics questions capture key accomplishments in implementing the NIPP risk management framework, Sector progress in key facets of the CIKR protection mission, and progress in achieving the goals identified in the Energy SSP. For 2008, the consolidated metrics will also include an examination of Sector partnerships that will emphasize gauging the health and effectiveness of Sector governance and coordination with security partners.

6.1.1 Building and Strengthening Partnerships

The Energy Sector continues to build and strengthen the role of existing CIKR protection partnerships entities, such as the GCC, SCCs, CIPAC, and energy security committees and working groups. Both the Energy GCC and the two Energy SCCs are well established and functioning at a high level. The Oil and Natural Gas SCC meets four times a year, while the Electricity SCC meets as needed and holds several meetings a year in conjunction with NERC CIPC events held around the United States and Canada. Membership in the Energy GCC has expanded to include power marketing administrations, and an additional trade group has joined the Oil and Natural Gas SCC. The Energy GCC continues to provide for close cooperation

among representatives from State and local governments and for participation from a tribal representative.

The Oil and Natural Gas SCC, together with the Chemical Sector, has established an EM Working Group that will work with DOE during energy emergencies to facilitate communication and cooperation between the two sectors. Furthermore, the Oil and Natural Gas SCC Working Group is developing and using HSIN-ONG.

6.1.2 Effective Communication with Security Partners

A number of the Energy Sector's ongoing activities are aligned with the first goal listed in the Energy SSP: Establish robust situational awareness within the Energy sector through timely, reliable, and secure information exchange among trusted public and private sector security partners. During the past year, DOE's secure ISER Web site, ISERnet, was significantly enhanced to facilitate communication and information exchange during energy emergencies for Emergency Support Function (ESF)-12 responders and other sector partners. The Energy Sector has also actively participated in many exercises (e.g., Eagle Horizon and TOPOFF).

Several initiatives are in place for information exchange within the Electricity and Oil and Natural Gas Subsectors. The Oil and Natural Gas SCC has established an Emergency Response Working Group, while the NERC CIPC provides excellent connectivity to Electricity Subsector security partners. The Electricity Subsector also uses its Information Sharing and Analysis Center to share information.

Further, DOE maintains and updates emergency contact lists through the HSIN and ISERnet, as appropriate. DOE's energy situation reports are broadly shared with State, local, and industry partners through ISERnet and with other government agencies through HSIN.

6.1.3 State, Local, Tribal, and Territorial Activities

Several DOE and DHS efforts are underway to work with representatives from State, local, tribal, and Territorial governments in supporting protective and resiliency programs. These representatives, along with Energy Sector members from Canada, participate on the Energy GCC. Efforts at regional levels include holding workshops and exercises and providing targeted communication to State and local officials through ISERnet.

6.1.4 Cross-sector Efforts

The Energy Sector has actively worked to obtain a better understanding of the interdependencies among CIKR sectors, including Transportation Systems, Banking and Finance, and Communications, which was a gap identified in the 2007 Energy Sector Annual Report. DOE is examining interdependency issues, such as Energy Sector water use and its possible impacts and pandemic planning through NISAC. In addition, DOE participated in a high-level HHS exercise

that incorporated energy issues and concerns. DOE also shares its work on visualization and modeling with cross-sector security partners and routinely shares products from other efforts with the Banking and Finance Sector and with HHS during energy-related emergencies.

Moreover, the Energy Sector regularly meets with agencies in the EPA (Water Sector), Treasury Department (Banking and Finance Sector), Federal Communications Commission (Communications Sector), and with other federal agencies to share approaches and effective security practices related to infrastructure protection, restoration, and recovery.

Finally, other CIKR sectors are becoming increasingly aware of the critical role energy plays in their operations, and DOE has been participating in several GCC groups, including the Chemical, Transportation Systems, and Healthcare and Public Health sectors's GCCs.

6.1.5 Protecting International Energy Assets

International terrorism, combined with increasing energy consumption by developing nations, continues to put upward pressure on energy prices worldwide. DOE identified this energy supply vulnerability as a gap in the 2007 Energy Sector Annual Report and has undertaken several initiatives to improve energy security through CIP beyond national borders. For example, in cooperation with DHS and the Department of State, DOE has established a team to work with international partners to conduct assessments and improve the protection of critical assets abroad. The team works with the Department of State on issues related to energy security. DOE is also collaborating with DHS on identifying critical energy sector assets abroad that could have a significant impact on the United States, and it has participated in an assessment of an LNG facility in Trinidad and Tobago.

6.1.6 DOE and DHS Collaborations

DOE works with DHS IP to ensure that DHS programs target any significant energy assets that have been identified. DOE and both the Oil and Natural Gas Subsector and the Electricity Subsector have cooperated in implementing CFATS. In support of DHS's increased emphasis on CIKR education and awareness, DOE, in coordination with Energy Sector partners, developed a "For Official Use Only" version of the Energy SSP that has been widely distributed to Sector partners, and a redacted public version has been made available through the Internet. DOE, through the Energy GCC and the two SCCs, reviewed the Energy SSP and decided that an update is not needed at this time.

In summary, the Energy Sector continues to make considerable progress toward accomplishing the goals and objectives in the NIPP and Energy SSP. Its accomplishments and the descriptions of CIKR protection activities, projects, and tools compiled from metrics data reveal its emphasis on Sector partnerships and collaboration. The Energy Sector will continue to develop and expand the constructs established through the NIPP partnership model to effectively coordinate and share information with Energy Sector and cross-sector security partners. The focus on developing an integrated approach and a robust set of CIKR protection programs has provided

the foundational elements needed to progress in the mission area and adapt to new CIKR protection challenges.

6.2 Path Forward

DOE plans to continue to work closely with its Energy Sector security partners to meet the milestones outlined in the Energy SSP. In 2009, DOE and its partners will reexamine the plan and determine if and how it might be updated and improved.

Specifically, DOE plans to:

- Lead the national effort to enhance energy infrastructure security and reliability in order to realize a reliable, survivable, and resilient energy infrastructure, in partnership with the Energy GCC and Oil and Natural Gas and Electricity SCCs.
- Work with Sector partners in reexamining the NIPP to improve and refine it.
- Further cooperate with its partners and with sectors that are of critical importance to the Energy Sector, with a focus on reliability, survivability, and resiliency.
- Work with Energy Sector partners to avoid or reduce duplication of effort and implement cost-effective approaches to achieve mutual goals.
- Participate on other energy-related national sector GCCs and working groups, and the State, Local, Tribal, and Territorial GCC and working groups.
- Participate in the Metrics Working Group involving representatives from all CIKR sectors.
- Provide consultation and assessments of facility security operations and security force training to State, local, and tribal (as well as foreign) entities in relation to critical global energy facilities and systems.
- Work with Energy Sector security partners to collaboratively develop requirements for sharing information. Collaborate with DHS to provide Energy Sector CIKR through a process for communicating incidents that is simple and rapid and facilitates incident reporting and the flow of information about response resources.
- Develop an electronic knowledge-based data aggregation and visualization capability to improve situational awareness.
- Lead the Energy GCC and Subsector SCCs in cooperating with DHS to develop and implement a CIKR training and education strategy.

- Work with the Energy GCC and Subsector SCCs in sponsoring training conferences, seminars, symposiums, and workshops for Energy Sector security partners.

- Work with Energy Sector security partners to identify systemwide vulnerabilities in power, fuel, and other key sector assets and to develop plans and approaches to secure and reconstitute those assets.

- Develop tools and mitigation solutions to help Energy Sector owners and operators improve resiliency and implement effective security practices.

- Continue to develop deployable analysis capabilities for use during emergencies that offer both predictive and post-event evaluations of the effects of a disruption in the energy system to the government and private sector partners in the field.

- Collaborate with Energy Sector CIKR owners and operators to support the development of comprehensive emergency, disaster, and continuity-of-operations plans.

- Identify and manage the risks associated with supply chain and other infrastructure dependencies that could affect Energy Sector CIKR.

- Update the State Energy Assurance Guidelines and develop local government energy assurance guidelines to help cities, counties, and municipalities better prepare for and respond to energy disruptions and emergencies.

- Continue to develop sector-specific metrics that help describe, in quantitative terms, the progress the Energy Sector is making in reducing risk, from the perspective of owners and operators. The Energy Sector Metrics Working Group will develop a draft set of sector-specific metrics, and members of the SCCs and the Energy GCC will review, revise, and approve them. During this time, the Energy Sector may hold workshops that help identify what security measurement practices and metrics are considered most effective by owners and operators. The Sector will have an approved set of metrics by May 2009 and some initial data by May 2010, assuming that various issues of concern can be successfully addressed. The Sector will draw upon existing data sources to the greatest extent practical.

This page intentionally blank

Attachment A: Acronym List

AGA	American Gas Association
AMS	Area Maritime Security (Plan) (USCG)
AMSC	Area Maritime Security Committee (USCG)
APEC	Asia Pacific Economic Cooperation
APGA	American Public Gas Association
API	American Petroleum Institute
APPA	American Public Power Association
ASP	alternate security program
Bcf	billion cubic feet
Bcf/d	billion cubic feet per day
BPA	Bonneville Power Administration
BZP	Buffer Zone Program
BZPP	Buffer Zone Protection Plan
C/ACAMS	Constellation/Automated Critical Asset Management System
CCIR	Commander's Critical Information Requirements (USACE)
CFATS	Chemical Facility Anti-terrorism Standards (DHS IP)
CFE	Comisión Federal de Electricidad
CFR	*Code of Federal Regulations*
CII	critical infrastructure information
CIKR	critical infrastructure and key resources
CIP	critical infrastructure protection
CIPAC	Critical Infrastructure Partnership Advisory Council (NIPP)
CIPC	Critical Infrastructure Protection Committee (NERC)
CMTS	Committee on the Marine Transportation System (DOT)
COI	chemical of interest
CR	comprehensive review
CSAT	Chemical Security Assessment Tool
CSR	Corporate Security Review (Program) (TSA)
DATES	Detection and Analysis of Threats to the Energy Sector (Project)
DEED	Demonstration of Energy-Efficient Developments (Program) (APPA)
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOI	U.S. Department of the Interior
DOT	U.S. Department of Transportation
EEAC	Energy Emergency Assurance Coordinators (System) (DOE OE)
ECIP	enhanced critical infrastructure protection (DHS IP)
EEI	Edison Electric Institute
EIA	Energy Information Administration (DOE)

EIAC	Energy Industry Assurance Coordinators (System) (DOE OE)
EM	emergency management
EMWG	Emergency Management Working Group
EOC	emergency operations center
EPA	U.S. Environmental Protection Agency
EPCA	Energy Policy and Conservation Act
EPRI	Electric Power Research Institute
ERCOT	Electric Reliability Council of Texas
ERO	Electric Reliability Organization
ERP	emergency restoration plan
ESF	Emergency Support Function
ESISAC	Electricity Sector Information Sharing and Analysis Center (NERC)
ESSP	Energy Sector-Specific Plan
FBI	Federal Bureau of Investigation
FCO	Federal Coordinating Officer
FE	Office of Fossil Energy (DOE)
FEMA	Federal Emergency Management Agency (DHS)
FERC	Federal Energy Regulatory Commission
FMSC	Federal Maritime Security Coordinator (USCG)
FSA	facility security assessment
FSO	Federal Security Officer (USCG)
FSP	facility security plan
FY	fiscal year
GCC	Government Coordinating Council
HITRAC	Homeland Infrastructure Threat Risk and Analysis Center (DHS)
HAS	Homeland Security Advisor
HSDB	Homeland Security Data Base
HSIN	Homeland Security Information Network (NPRA)
HSIN-CS	HSIN for the Chemical Sector
HSIN-ONG	HSIN for the Oil and Natural Gas Subsector
HSPD	Homeland Security Presidential Directive
HSS	U.S. Department of Health and Human Services
iCAV	Integrated Common Analytical Viewer (DHS IP)
ICS	Incident Command System
IEA	International Energy Agency
IED	improvised explosive device
ieRoadmap	Interactive Energy Roadmap (DOE)
IESO	Independent Electric System Operator
IICD	Infrastructure Information Collection Division (DHS)
IFIP	Interagency Forum for Infrastructure Protection
ILTA	International Liquid Terminals Association
INGAA	Interstate National Gas Association of America

IP	Office of Infrastructure Protection (DHS)
ISAC	Information Sharing and Analysis Center
ISER	Office of Infrastructure Security and Energy Restoration (DOE-OE)
ISERnet	ISER's secure Web site
IT	information technology
ITSF	Information Technology Security Forum (API)
LAR	Los Angeles Refinery
LNG	liquefied natural gas
Mcf	million cubic feet
MMS	Minerals Management Service (DOI)
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
NAEWG	North American Energy Working Group
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Officials
NCP	National Contingency Plan
NCSD	National Cyber Security Division (DHS)
NCSL	National Conference of State Legislatures
NERC	North American Electric Reliability Corporation
NETL	National Energy Technology Laboratory
NGA	National Governors Association
NG MARC	Natural Gas Mutual Aid Resource Center (AGA)
NGSC	Natural Gas Security Committee (AGA)
NIAC	National Infrastructure Advisory Council
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan (DHS)
NISAC	National Infrastructure Simulation and Analysis Center
NNL	Pacific Northwest National Laboratory
NPRA	National Petrochemical and Refiners Association
NRCAN	Canadian Department of Natural Resources
NRECA	National Rural Electric Cooperative Association
NRF	National Response Framework
NRP	National Response Team
NSTB	National SCADA Test Bed (Program) (DOE-OE)
NVIC	Navigation and Vessel Inspection Circular
NWPP	Northwest Power Pool
OCS	Outer Continental Shelf
OE	Office of Electricity Delivery and Energy Reliability (DOE)
OMB	Office of Management and Budget
OPS	Office of Pipeline Safety (DOT)
OQ	operation qualification

QI	qualified individual
PCII	Protected Critical Infrastructure Information (Program)
PCIS	Partnership for Critical Infrastructure Security (DHS)
PCSR	Pipeline Corporate Security Review
PFO	Principal Federal Official
PHMSA	Pipeline and Hazardous Materials Safety Administration (DOT)
PMAs	Power Marketing Administrations (DOE)
PNCA	Pacific Northwest Coordination Agreement
PNWER	Pacific Northwest Economic Region
PSA	Protective Security Advisor
PSEPC	Public Safety and Emergency Preparedness Center
PTI	Public Technologies Institute
R&D	research and development
RAM-T^{SM}	Risk Assessment Methodology for Transmission (BPA)
RBPS	risk-based performance standard
RMA	Response Management Associates, Inc.
RP3	Reliable Public Power Provider (Program) (APPA)
RTF	Reliability Task Force (NRECA)
RTO	regional transmission organization
RUS	Rural Utilities Service (USDA)
S&T	Science and Technology (Directorate) (DHS)
SAV	site assistance visit
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Council
SIF	Security & Integrity Foundation
SLTT GCC	State, Local, Tribal, and Territorial Government Coordinating Council
SPCC	spill prevention control and countermeasures
SPP	Security and Prosperity Partnership for North America
SPR	Strategic Petroleum Reserve
SSA	Sector-Specific Agency
SSCP	Secure SCADA Communications Protocol
SSP	Sector-Specific Plan
STEP	Spare Transformer Equipment Program
STQ	screening threshold quantity
SVA	security vulnerability assessment
SWPA	Southwestern Power Administration (DOE)
SWRTA	Southwest Regional Transmission Association
TALON	Threat and Local Observation Notice (Model) (USACE)
TISP	The Infrastructure Security Partnership
TSA	Transportation Security Administration (DHS)
TSI	Threats and Suspicious Incidents (Program) (USACE)
TSWG	Technical Support Working Group

TVA	Tennessee Valley Authority
TWIC	Transportation Worker Identification Credentials (Program)
USACE	U.S. Army Corps of Engineers
US-CERT	U.S. Computer Emergency Readiness Team
USDA	U.S. Department of Agriculture
USCG	U.S. Coast Guard
VMWG	Visualization and Modeling Working Group (DOE-OE)
WECC	Western Energy Coordination Council
Western	Western Area Power Administration
WHO	World Health Organization
WMD	weapon(s) of mass destruction
WSCC	Western Systems Coordinating Council
WRTA	Western Regional Transmission Association

This page intentionally blank

Attachment B: Energy Sector Overview

HSPD-7 identified 18 CIKR sectors[15] and designated Federal Government SSAs for each one. Each sector is responsible for developing and submitting SSPs and sector-level performance feedback to DHS to enable it to assess gaps in the national cross-sector CIKR protection program. SSAs are responsible for collaborating with private sector security partners and encouraging the development of appropriate information-sharing and analysis mechanisms within the sector.

B.1 Description of the Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, the health and welfare of the Nation is threatened, and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector. The energy infrastructure is divided into three interrelated segments: electricity (Electricity Subsector), petroleum, and natural gas (Oil and Natural Gas Subsector).

The U.S. Electricity Subsector contains more than 5,300 power plants with about 1,075 gigawatts of installed generating capacity. About 49 percent of the electricity is produced by combusting coal (primarily transported by rail), 19 percent is produced in nuclear power plants, and 20 percent is produced by combusting natural gas. The remaining generation is provided by hydroelectric plants (7 percent), oil (2 percent), and renewable (e.g., solar, wind, and geothermal power) and other sources (3 percent). Electricity generated at power plants is transmitted over 211,000 miles of high-voltage transmission lines. Voltage is stepped down at substations before being distributed to 140 million customers over millions of miles of lower-voltage distribution lines. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators that use sophisticated energy management systems that are supplied by SCADA systems to keep the system in balance.

In the U.S. Oil and Natural Gas Subsector, the Petroleum Subsector (i.e., oil portion) entails the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the United States. Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, liquefied petroleum gases, and basic petrochemical feedstocks. Both crude oil and petroleum products are imported, primarily by ship, as well as being produced domestically. Currently, 66 percent of the crude oil required to fuel the U.S. economy is imported. In the United States, there are more than 500,000 wells producing crude oil, 30,000 miles of gathering pipeline, and 51,000 miles of crude oil pipeline. There are 149 operable petroleum refineries, 116,000 miles of product pipeline, and 1,400 petroleum terminals. Petroleum also relies on sophisticated SCADA and other systems to control production and distribution; however, crude oil and petroleum products are stored in tank farms and other facilities.

15 An 18th sector (Critical Manufacturing Sector) was added in 2008.

Natural gas is also produced, piped, stored, and distributed in the United States. Imports of LNG are increasing to meet growing demand. There are more than 448,000 gas production and condensate wells and 20,000 miles of gathering pipeline in the country. Gas is processed (impurities removed) at more than 550 operable gas processing plants, and there are almost 302,000 miles of interstate and intrastate pipeline for the transmission of natural gas. Gas is stored at 399 underground storage fields and 103 LNG peaking facilities. Finally, natural gas is distributed to homes and businesses in more than 1,175,000 miles of distribution pipelines. The Natural Gas subsector's heavy reliance on pipelines highlights its interdependency with the Transportation Systems Sector, and it relies on the Electricity Subsector for power.

B.2 Sector Partnerships

DOE will coordinate with sector information-sharing organizations through the HSIN and other approaches, as well as with other concerned organizations (e.g., FERC, NERC, NARUC, and NASEO) and the governments of Canada and Mexico, to share energy infrastructure information and plan exercises that address energy infrastructure issues.

On August 8, 2005, President Bush signed the Energy Policy Act of 2005 into law. It requires the implementation of mandatory electricity reliability standards in the United States. The implementation of these standards will be paralleled by implementation in Canada. Ongoing responsibility for monitoring and reporting with respect to implementing the recommendations for following up on the 2003 Northeast Blackout will be assumed by a joint U.S./Canada oversight group.

The Energy Sector has been proactive in developing and implementing security programs to support CIKR protection. The Electricity and Oil and Natural Gas Subsectors and other government sectors have continued to develop programs and initiatives to advance CIP goals and priorities.

DOE and other Federal, State, and local government agencies have been working with their security partners — public and private utilities — through the Oil and Natural Gas SCC and Electricity SCC to better secure CIKR across the Nation.

The Electricity SCC represents more than 95 percent of Electricity Subsector owners and operators and has been meeting on a regular basis to discuss the SSP and other security initiatives. The Oil and Natural Gas SCC represents more than 98 percent of Oil and Natural Gas Subsector owners and operators. This council, formed by oil and natural gas trade associations, serves as a broad, industrywide network to help coordinate ongoing industry initiatives, government partnerships, and responsibilities. It selects a representative from the industry to serve as chair and act as the liaison to DHS.

An Energy GCC was established in early 2004; it is co-chaired by DHS and DOE. It consists of Federal Energy Sector-related organizations, as well as representatives of State and local governments. The Energy GCC has met with its SCC counterparts to share information. Under CIPAC (which reports to the Secretary of Homeland Security), the Energy GCC, Electricity

SCC, and the Oil and Natural Gas SCC have formed joint working groups that are dedicated to protecting the Nation's critical energy infrastructure.

This page intentionally blank

Attachment C: Energy Sector-Specific Plan Pandemic Planning

Business continuity planning for the Energy Sector requires a lot of preparation and consideration of the full range of threats facing system owners and operators. The sector's business continuity plans have been effective so far. However, these plans consider classic scenarios, such as man-made disasters, common natural disasters (e.g., floods, hurricanes), and loss of infrastructure (e.g., systems, power). Recent concerns over the possibility of a pandemic and its potential impacts has encouraged both the government and industry to make plans to prepare for a possible threat of pandemic influenza, building on the efforts already taken by various groups within the Energy Sector.

Energy Sector owners and operators have been encouraged to enhance their business continuity plans to meet the threat of pandemic influenza and should integrate them with other existing plans for effective enterprise-wide recovery. The Electricity Subsector, Oil and Natural Gas Subsector, and other agencies and organizations within the Energy Sector have already begun to plan and prepare for the possibility of pandemic influenza.

Reference guides for planning, preparation, and response are available to help Energy Sector members develop plans to manage the threat to the sector's business continuity. Draft DHS guidelines can be found in two attachments included here: attachment C.1, "Annex: Electricity Subsector Pandemic Influenza Guideline" and attachment C.2, "Annex: Oil and Natural Gas Subsector Pandemic Influenza Guideline." These annexes are from the DHS 2003 publication, *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* (i.e., CIKR Pandemic Guide). Each guideline builds on industry efforts. (Examples are NERC's *Electricity Sector Influenza Pandemic Planning, Preparation, and Response Reference Guide,* which can be accessed at ftp://www.nerc.com/pub/sys/all_updl/cip/Influenza%20Pandemic%20Reference%20Guide.doc, and API documents on the oil and gas industry.) The guidelines are practical tools that can be used to tailor and enhance existing emergency response plans to address unique challenges like pandemic influenza. For each subsector, the guidelines suggest a relevant action, supporting action, and question to consider, which can be integrated and managed as separate checklist items during planning. Actions are the primary checklist items; each one has several related supporting actions and questions to consider. Supporting actions expand on the overarching action by suggesting issues to examine further. Questions to consider are sector-specific questions that focus on the main and supporting actions. Overarching categories covered in these guidelines are as follows: essential services and functions, essential systems and equipment, essential raw materials and supplies, essential workers, essential interdependencies, and regulatory issues and impacts from community disease-mitigation strategies. The Energy Sector's guidelines will be integrated with those for each of the other CIKR sectors in a new Annex to the CIKR Pandemic Guide.

NERC and other Electricity Subsector partners have formed a task force to develop a reference guide and revise it as necessary. Associations such as the AGA have representatives from the petroleum and natural gas production, transportation, and distribution industries who are participating in a DHS program to develop and validate sector-specific pandemic planning

guidelines. The AGA is also participating in the DHS and HHS NIAC task group. This group is developing recommendations on pandemic countermeasures and on how to prioritize the distribution of vaccines and antiviral medications to critical infrastructures. The AGA has also identified and established single points of contact to serve as the conduit for pandemic information.

The World Health Organization (WHO) has identified six pandemic phases, which include the inter-pandemic, pandemic alert, and final pandemic periods. These phases, along with the Federal Government response phases, are described in attachment C.3, "WHO Pandemic Phases and the Federal Government Response Stages." They were included in the "Oil and Natural Gas Subsector Pandemic Influenza Guideline" (attachment C.2). In brief, in the inter-pandemic period, no new influenza virus subtypes have been detected in humans, but an influenza virus subtype may be present in animals and pose a risk of human disease. In the pandemic alert period, a human infection(s) with a new subtype is present and begins with no human-to-human contact. Then smaller and then larger clusters become prevalent, and human-to-human contact is spreading but localized. In the final pandemic period, there is increased and sustained transmission in the general population. These phases give businesses a useful framework on how to plan for a pandemic. However, pandemic response plans should first be coordinated with the appropriate Federal, State, local, and provincial government agencies. Organizations such as NERC have adjusted the WHO phases for their own use in business continuity planning for the Electricity Subsector.

NERC's reliability standards can be seen in attachment H, which lists the phase (i.e., planning, preparedness, response, or recovery, or one of an organization's specific, adjusted, relevant phases) to which each key action corresponds. The assignment of responsibilities and due dates helps in defining a more formal plan and makes individuals or teams within the organization accountable.

Through the NIPP and the "partnership model," government energy security partners are supporting industry efforts and building closer working relationships to address the interdependent aspects of a possible pandemic. DHS, through NISAC (Sandia and Los Alamos National Laboratories), is supporting modeling efforts, and government agencies are cooperating in a number of exercises to support improved cooperation.

In summary, the Energy Sector already has several efforts underway with regard to pandemic influenza that are useful to owners and operators. Progress is ongoing with regard to developing pandemic plans, guides, exercises, work groups, points of contact, and other items for the agencies and organizations that make up this sector. This work is a continuing effort; although advances have been made, the Energy Sector will keep working to meet these objectives and make modifications as needed to address changes in the pandemic influenza threat.

Attachment C1: Annex — Electricity Subsector Pandemic Influenza Guideline

ANNEX: Electricity Subsector Pandemic Influenza Guideline

Purpose: This Sector-specific guideline is an annex to the *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* (*CIKR Pandemic Influenza Guide*) and intends to assist the Electricity Sector with its plan for a catastrophic pandemic influenza. Organizations that fail to prepare for such a prolonged catastrophic event may find themselves without the staff, equipment, or supplies necessary to continue providing electricity to their customers and the nation. For a copy of the complete CIKR Pandemic Influenza Guide, please see www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf.

How-to-Use Guidelines: This guideline serves as a *non-prescriptive* reference for owner-operators and a practical tool that business planners can use to augment and tailor their existing emergency response plans given the unique challenges a pandemic influenza presents. **It is important to integrate your pandemic influenza plan with business continuity and emergency response plans and/or the *CIKR Pandemic Influenza Guide's* comprehensive framework for pandemic influenza planning.** This annex addresses some of the unique challenges the Electricity Sector may face during an influenza pandemic, as well as the seven major areas of vulnerability the sector should fully assess in planning for pandemic influenza. These areas are *essential* to the planning process. **While not necessarily applicable to all businesses or entities in a given sector, each relevant *Action*, *Supporting Action,* and *Question* can be integrated and managed as a separate checklist item during the planning process.**

- **Actions**: These are primary checklist items with numerous related supporting actions and questions to consider.
- **Supporting Actions**: Expanding on the overarching action, these supporting actions offer suggestions for further study.
- **Questions to Consider**: These questions are Sector-specific and designed to focus on the main and supporting actions. These questions are not comprehensive; they simply represent a starting point to stimulate thinking about further actions and options. All sectors have similar primary/supporting actions; it is the questions asked and the unique attributes of each sector that discriminates the plans of one sector from another.

Planning Assumptions: Influenza pandemics are unpredictable, and it is impossible to forecast its characteristics or severity accurately. However, if a severe influenza pandemic emerges, given today's highly mobile population, outbreaks may occur nearly simultaneously across the country making reallocation of resources more difficult than with other emergencies. While an influenza pandemic will likely affect a given community for six to eight weeks, nationally a wave may linger for up to 12 weeks. Thus, even though a community outbreak may have subsided, businesses in those communities that depend on a national supply chain may find themselves without the necessary materials, supplies, and workforce because other communities across the country may still be affected by an outbreak. Therefore, each sector must rely primarily on its own internal resources for response. The guidance, which is based on disease impact assumptions (pandemicflu.gov/plan/pandplan.html) from the Centers for Disease Control and Prevention (CDC), includes the following:

- *Susceptibility to the pandemic influenza virus will be universal.*
- *Once person-to-person transmission begins, the disease will spread rapidly around the globe.*
- *The clinical disease attack rate will likely be 30 percent or higher in the overall population during the influenza pandemic.*
- *Rates of absenteeism will depend on the severity of the influenza pandemic. In a severe influenza pandemic, absenteeism attributable to illness, the need to care for ill family members, and fear of infection may reach 40 percent during the peak weeks of a community outbreak.*
- *Pandemic influenza waves will last 6-8 weeks in affected communities and up to 12 weeks nationally.*

For detailed information on the complete set of planning assumptions and the pandemic influenza context, see Section 3 of the CIKR Pandemic Influenza Guide and the other Federal guidance at www.pandemicflu.gov.

ESSENTIAL SERVICES AND FUNCTIONS

Industries in all sectors of the American economy will experience pandemic influenza impacts – the Electricity Sector is no exception. The Electricity Sector's essential functions and services include generating electricity, coordinating its distribution, and communicating and receiving payment from customers. Electric generation accounts for 40 percent of energy consumed in the U.S. All CIKR sectors depend on electricity and any interruption in supply would cause significant damage to the U.S. economy and the American people.

ACTION **Identify and assess essential services and functions.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify essential services that must keep operating and the critical functions needed to support those services (e.g., control rooms, power plant operations, system switching).	• Can you maintain essential services and functions given the potential 40 percent absenteeism during an influenza pandemic? • What functions and processes must you sustain to produce, distribute, and maintain critical services and functions? • Who are your critical customers? Can you prioritize essential services/functions to serve critical customers (e.g., hospitals)? If so, can you deliver electricity to them independently of your other customers? • Have you communicated with your service providers, suppliers, government entities, health care providers, and critical customers about the need to jointly plan for an influenza pandemic? • Have you revised your incident management capabilities to address a pandemic influenza threat? • Have you devised plans to accommodate for the impact of suspending certain operations? • Have you established alternatives to assure cash transactions with the public are minimized? • Have you identified alternative fund-transfer means should the pandemic influenza impact usual mechanisms (banking) for funding suppliers and paying employees?
❑	Identify services and functions (e.g., meter reading, training) that you can suspend.	
❑	Prioritize essential services and functions given their value to your critical customers and the community.	
❑	Assess remote connectivity and accessibility options for workers to ensure products and services remain operational.	

ESSENTIAL SYSTEMS AND EQUIPMENT

Unlike other disasters, an influenza pandemic will not physically damage infrastructure. However, planners must assess the impact that personnel loss (attributable to illness, the need to care for ill family members, fear of infection and death) will have on reduced or delayed maintenance of essential systems or equipment. Additionally, an influenza pandemic's impact on the supply chain (i.e., "just-in-time delivery, warehousing, and logistics) could limit your ability to receive replacement parts and supplies, or to conduct routine maintenance for an extended period. Plans should address contingencies and their impacts on primary and supporting essential equipment. Organizations that rely on remote real-time services to maintain continuity should consider adjusting their telecommuting activities to make them more efficient. A list of essential systems and equipment will likely include: transmission and distribution lines, transmission and distribution substations, control centers and supporting systems, customer call centers, and control systems.

ACTION **Review systems and equipment critical to support each essential function.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify equipment that must operate continuously and/or at key periods to sustain essential functions and processes.	• Can you modify equipment and processes temporarily to maintain essential functions? • How will pandemic influenza-induced changes (e.g., increased call center traffic) affect operations and demand on essential equipment? • How will you maintain and repair essential equipment given potential supply chain issues? • Is your equipment clearly mapped and marked so it can be located in case of emergency repair or replacement by non-regular staff or others? • Have you developed standard operating procedures for your processes and equipment, and, if so, have you distributed them broadly to managers and staff? • To what extent has regular staff had cross training and therefore able to support another role if needed? • Do you have pre-established contracts with multiple equipment vendors for emergency replacement and repair during an influenza pandemic? • How do you plan to ensure hygienic conditions in mission critical areas used by multiple shifts (e.g., contracting with a cleaning company)? • Do you have sufficient backup personnel to maintain and repair essential equipment given that 40 percent of your workforce could be absent?
❑	Identify and prioritize safety/security requirements for maintaining essential equipment and assets.	
❑	Review primary and supporting components of critical equipment to identify potential single-point failures and possible cascading consequences.	
❑	Consider how each action relates to those actions in your organization's contingency plans to address other emergencies.	

ACTION	Prepare to sustain essential equipment for a wave lasting up to 12 weeks.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Prioritize available options to reduce demands on your resources.	• Is there excess operational capacity for your essential equipment to sustain functions while alternating and reducing demands on specific equipment and workers (e.g., technology to support remote operations)? • Do you have replacements available for essential equipment either on-site or locally? • Is your regular routine maintenance on your essential equipment up-to-date, and how much routine maintenance is required for this equipment? • Do you have updated standard operating procedures for this equipment, and have you changed them to address pandemic influenza conditions (e.g., social distancing strategies)? • Can you defer or accelerate scheduled maintenance on short notice? • Have you considered how you will maintain essential services and functions if another disastrous event (such as a hurricane or ice storm) affects your critical systems/equipment during a wave? • Can you maximize use of equipment/processes that can function via remote access?
❑	Assess recurring and preventative maintenance requirements.	
❑	Assess implications if essential equipment fails early on in an influenza pandemic.	
❑	Join with a mutual aid and assistance program to assist with essential equipment, noting that traditional mutual aid assistance networks may not be available or will be severely limited during an influenza pandemic.	

ESSENTIAL RAW MATERIALS AND SUPPLIES

A pandemic influenza wave may linger in a community for six to eight weeks and for up to 12 weeks nationally. The negative impacts on individuals, organizations, and the nation from the illness and disease mitigation strategies will have an effect over a much longer duration than other typical disasters. A severe influenza pandemic may disrupt access to your essential materials and supplies necessary to function for up to 12 weeks. Operators should explore their supply chains, beginning with internal storage capacity and tracking along the network to the source of the materials. Given an increased reliance on "just-in-time" delivery and potential impacts that could shut down the supply chain, you may consider stockpiling fuels (coal, gas, and oil), replacement parts, and infection control supplies (e.g., hand sanitizer, cleaning supplies) on-site or locally or make other contingency plans.

ACTION **Identify materials and supplies to sustain essential functions and equipment for up to 12 weeks.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify the critical fuels needed to provide power continuity.	• How can you expand fuel stockpiles to sustain essential operations for up to 12 weeks in case supply chain production and/or delivery challenges develop? If expanding stockpiles is not a practical option, how can you plan to sustain your operations given that deliveries of fuel will be reduced or become more sporadic? • What happens if your supply chain cannot provide critical materials or supplies? • Will advance notice of supply-chain disruption be available? Will it be sufficient to switch suppliers or take plants offline? • Do you have sufficient stocks of personal protective equipment and cleaning supplies to ensure high levels of hygiene in common work areas that will be used by personnel required to maintain essential services? • Do critical systems have replacement parts on-site for maintenance?
❑	Prioritize essential material and supplies necessary to operate equipment and sustain essential functions.	
❑	Identify options to reduce demand for essential supplies and materials.	
❑	Explore options for expanding stockpiles and close-by storage.	
❑	Assess internal and external supply-chain support operations and contracts.	

ACTION	Determine the most effective ways to ensure an adequate supply of essential materials.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Assess costs to procure, stock, and/or ensure delivery of essential materials.	• Currently, what is the level of fuel stockpile you have available? Can you calculate the cost of expanding your stockpile to cover a 12-week pandemic influenza wave? • Can you fund an expansion of fuel supplies? Are special financing methods warranted? • Where can additional supplies be stored if on-site capacity is limited and/or at capacity? • Are there additional security constraints with off-site storage of supplies? • If you cannot stockpile critical materials or your "just-in-time" supply chain fails, do you have effective backup plans (e.g., pre-negotiated contracts with other suppliers for priority/emergency deliveries)? • Have you integrated your planning with your local/regional suppliers to ensure your organization is receiving priority support? • How can you provide incentives for your support contractors to become better prepared (e.g., collaborate on planning, integrate preparedness training, and stipulate pandemic influenza planning and certification in supply contracts)?
❑	Identify physical or safety limitations in stocking sufficient critical supplies locally.	
❑	Identify a formal chain of command to ensure someone is available to authorize major emergency procurements.	
❑	Identify additional security needs for increased high-value material stockpiles.	
❑	Coordinate with critical supply-chain vendors, and identify secondary sources for critical supplies.	

ESSENTIAL WORKERS

A severe influenza pandemic may generate extended absences for essential workers that might affect you and your supply chain. During an influenza pandemic the actual level of workforce absenteeism could reach 40 percent. To complicate matters, the disease will strike randomly among employees from operation managers to front-line workers, and it will also affect employee's family members. Implementing rigorous personal hygiene and social distancing strategies along with the strategic use of Personal Protective Equipment (PPE) in the workplace may reduce the impact of a potential worker-related crisis. A list of your most essential workers will likely include: control center operators, transmission line repair workers, call center operators, maintenance/repair specialists, and business and operational support.

ACTION **Identify the types and numbers of workers critical to sustain essential functions.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify essential workers based on ability to sustain essential equipment/functions.	• Have you identified the workers who are essential to sustain the essential functions and equipment necessary to produce your most essential goods and services? • Are there constraints in employing union contract workers and/or for specific local worker contracts in non-standard ways during an emergency temporarily (e.g., can a skilled maintenance technician temporarily serve as an operator)? • What different challenges do you face with modifying standard tasks and/or supporting or replacing full-time versus part-time or seasonal employees? • To what extent has regular staff had cross training and therefore able to support another role if needed? • Are there differences in your workforce by age and/or family status (e.g., employees with younger children may be affected more by school closures and self-quarantine)? • What are the different challenges for on-site vs. off-site and full vs. part-time contractors? • What essential operations might you support temporarily through external contract support and how prepared are these support contractors for an influenza pandemic?
❑	Establish clear roles and responsibilities of employees, labor organizations, staff, supervisors, and managers.	
❑	Assess impacts from an extended absence by essential workers.	
❑	Assess your options to obtain contractor backup support on essential operations and determine how quickly that can be started.	

ACTION	Identify policies and procedures to ensure a safe workplace.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Emphasize worker/workplace disease control and protection. For more information, see: www.pandemicflu.gov/plan/workplaceplanning/index.html.	• Have you considered the possibility of sending home non-essential staff to reduce the chance for disease introduction and transmission? • Have you considered the need and conditions for more extreme measures, such as sequestering on-site the most essential staff? • How do you fund the costs associated with stocking worker protection items such as PPE? • Have you established a process for your occupational health nurse to follow up on sick employees? • Have you considered closing or restricting use of non-critical common areas, such as exercise rooms and cafeterias? • Have you considered the need or the ability to completely separate staff and customers/visitors while performing functions? • If you are not the owner or only occupant of a facility, have you factored the facility's pandemic influenza plan into yours? Have you coordinated your critical actions with their's and ensured that there are no conflicting policies and recommendations?
❑	Determine the types of PPE best suited for your various workers. For suggestions, see: www.osha.gov/Publications/nfluenza_pandemic.html.	
❑	Develop protocol (i.e., seek medical attention, avoid workplace, notify supervisor) for employees to follow if they contract the virus, show symptoms, or have ill family members.	
❑	Consider screening employees and visitors at the entrances to your critical facilities.	
❑	Consider limiting workplace access to visitors and other non-essential workers.	

ACTION	Identify policies and procedures to protect and sustain workers during an influenza pandemic.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Reduce demands on essential workers.	• Are there practical temporary changes you can take to increase essential worker availability (e.g., extending shifts to 12 hours, adding overtime, and using other non-essential workers)?
❑	Temporarily augment essential worker ranks.	• Are there recent retirees or other pools of workers who can help you in an emergency?
❑	Consider, where practical, plans to have an increased number of employees work from a safer off-site location (i.e., home).	• Have you cross-trained non-essential workers to perform essential jobs in an emergency? • Could you employ off-site work options for part of your staff (e.g., call center, human resources, and accounting staff)?
❑	Develop protocols (i.e., seek medical attention, avoid workplace, notify supervisor) for employees to follow if they contract virus, show symptoms, or have ill family members.	• Are your telecommunications and information technology infrastructure capable of shifting calls, data and other services off-site?

ACTION	Identify Human Resource (HR) protective actions and policies to sustain essential workforce.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Assess standard HR policies and procedures.	• Have you adapted existing or developed new sick leave policies to support ill workers and workers with ill family members (www.pandemicflu.gov/plan/community/commitigation.html)?
❑	Develop additional HR policies specific to pandemic influenza response.	• Have you met with unions and other HR groups on implementing new policies temporarily?
❑	Identify likely legal considerations that may arise from these new HR actions.	• Have you communicated with workers and their families about potential HR policy changes?
❑	Develop plans and procedures that provide support and assistance to employees' families.	• Have you identified possible actions to help reduce potential abuse of the leave policies?
❑	Provide regular communication to staff on the latest health advisories and recommendations regarding pandemic influenza.	• Have you noted legal ramifications (e.g., costs) of emergency HR and leave policies?
		• Have you consulted with health authorities to update confidentiality policies in order to manage employees who have potentially been exposed?
		• Health Insurance Portability and Accountability Act (HIPAA) means specific employee health status information may need to be protected. Has this been considered?
		• Have you developed/updated workforce deployment policies regarding teams and crews working together and potential need to keep employees separated?
		• Have you developed a staff travel policy, including possible provisions for quarantine after returning from an infected area? This would apply to work and non-work related travel.
		• Have you considered relevant Federal, State, or local laws (e.g., FMLA www.dol.gov/esa/whd/fmla/) that govern extended leave for employees?

ESSENTIAL INTERDEPENDENCIES

When an influenza pandemic strikes, it will affect all CIKR sectors. Preparedness activities require coordinated actions by Federal, State, and local government agencies as well as private sector entities that operate approximately 85 percent of the nation's infrastructure. To facilitate a swift pandemic influenza response and recovery, individual owners and operators of the Electricity Sector must identify and sustain their essential interdependencies within and across sectors. The nation's critical infrastructure relies on electricity for their essential functions. The Electricity Sector relies on the Oil and Natural Gas, Transportation, Communications and Finance sectors to provide raw materials necessary to generate electricity, coordinate its distribution, and communicate and receive payment from customers.

ACTION **Identify interdependent relationships and take actions to sustain this support.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Assess materials and modes of transportation used to deliver your raw materials (e.g., coal delivered by rail).	• What are the raw materials needed to produce electricity and does your supplier have a pandemic influenza plan in place to continue to provide those materials? • What other interdependencies might exist that are critical to your operations for which you depend on an outside organization? Will they be able to meet your needs in a pandemic? • How are your raw materials and supplies delivered to you, and will these transportation systems continue a reliable supply of materials during an influenza pandemic? • If communications networks fail or become unreliable or slow, can you maintain contact with other suppliers, public sector partners, remote workers, customers, or other essential parties? • If information technology networks are impaired, will telecommuting still be a viable alternative? What will be your fall-back plan? • Are there alternatives (e.g., electronic payment) if an influenza pandemic disrupts usual payment collection options? • What safety or security requirements will pandemic influenza pose and have you coordinated with public safety officials and local government officials? • Do you participate in public and private pandemic influenza planning and response training exercises?
❑	Assess the capability of communication channels to function under stress of pandemic influenza environment.	
❑	Develop joint operational plans with key service providers, suppliers and customers in the public and private sectors.	
❑	Assess capability of mutual aid and assistance networks to reduce vulnerabilities.	

REGULATORY ISSUES

In response to pandemic influenza, the government may provide direct support in the form of vaccines, antiviral medications, and personal protection supplies for essential workers; priority and clearances for an organization's supply deliveries; on-site public safety and physical security augmentation. Indirect support may come from governmental relief such as waivers for key regulatory issues specific to a sector. *However, no organization should count on regulatory relief and/or waivers in its pandemic influenza planning.*

ACTION **Identify Federal/State/local regulatory regulations that may affect operations.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify regulations that, if temporarily modified, would reduce impacts on critical functions, resources, and workers.	• What potential regulatory issues might your organization need to address during pandemic influenza? • What temporary direct/indirect government actions may help or hinder your organization's ability to maintain its business continuity and/or delivery of essential services and functions? • Have you considered, and prepared for, impacts from potential government response actions and cross-jurisdictional differences in response (e.g., possible quarantine of specific communities; widespread or localized travel restrictions)? For example, can you ensure essential workers are able to get to work? • Have you communicated with State regulatory agencies about your pandemic preparedness efforts? • Have you considered providing a copy of your pandemic plan to the necessary Federal and State agencies? • Do the States in which you operate have a Pandemic Influenza Plan and how might actions considered within the State's plan potentially effect utility operations? • Are there potential temporary worker and workforce strategies you can use in response to regulatory challenges generated by pandemic influenza (e.g. credentialing and licensing of workers, extending work hours)? • What customer shut-off policies or even moratoriums might be adopted during the height of an influenza pandemic should it occur in winter in northern climates or summer in southern climates when air conditioning may be necessary for individuals that are ill?
❑	Identify direct/indirect government support options that may help sustain your organization or sector.	
❑	Communicate potential relief actions in advance to workers, supporting entities, insurers, and customers.	

IMPACTS FROM COMMUNITY DISEASE MITIGATION STRATEGIES

To reduce impacts from a pandemic flu, Federal, State, local, and tribal government authorities, as well as private-sector entities, may implement mitigation strategies, including: voluntary isolation; voluntary home quarantine; school closures; and social distancing of adults in the community and workplace. The public health and social distancing strategies may ultimately contain the disease and will reduce the risk of infection and death, but they also will have significant consequences for organizations in the Electricity Sector that must be managed carefully. For more information on possible community mitigation strategies, please see www.pandemicflu.gov/plan/community/commitigation.html, particularly Appendix 4, and Section 3 of the *CIKR Pandemic Influenza Guide*.

ACTION **Identify possible effects from mitigation strategies; take actions to reduce negative impacts.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Calculate effects of Community Mitigation Strategies (www.pandemicflu.gov/plan/community/commitigation.html) on your organization.	• What impacts will the strategies have on worker absentee rates (e.g., how will it affect your workers if schools/childcare facilities close for weeks at a time)? • What are the costs associated with expanding your sick leave policies?
❑	Assess trigger points of the CDC's Pandemic Influenza Severity Index to determine the timing and use of mitigation interventions. For more information, see: (www.pandemicflu.gov/plan/community/commitigation.html#IV).	• How can you survey your employees to identify who may need to stay home, telework, or work an alternate schedule to care for children dismissed from school or childcare? What are the privacy laws that should be taken into account? • What workplace social distancing measures can you implement (e.g., work-at-home options, off-site work locations, split working/meal shifts, reduced travel, and increased use videoconferencing and teleconferencing)?
❑	Communicate with employees on the current pandemic influenza situation/threat level, and establish trigger points that initiate specific actions within the organization.	• Have you met with your local leaders on the timing of measures, alerts, and implementation they are considering for the community at-large as well as potentially for your organization? • What are the demand changes to your organization when schools and/or businesses close?
❑	Coordinate with Federal, State, local agencies and acknowledge responsibilities and command-control authorities of all parties and how this work within the National Incident Management System (NIMS)	• Do you have plans and procedures to provide support and assistance to employee families? • Have you compiled a list of employee contact numbers and email addresses to assure communications during the influenza pandemic? • Has your organization established call-in numbers or a website where employees and customers can uniformly receive updates from management on the current situation?

		(Cont.) • Have you worked with local public health officials regarding the availability of antivirals or vaccines for staff members who perform critical functions? • Have you considered contracting with a Pharmaceuticals Distribution Manager (PDM) to help manage the legal and logistical aspects of procuring, storing and distributing any antivirals or vaccines that your organization secures? • Will you allow access to contractors, or other utilities that send mutual assistance personnel, to your service area if restoration assistance is required?

For additional useful information, including a PDF copy of the complete ***Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources***, visit www.pandemicflu.gov or email your questions to dhspandemic@dhs.gov.

This page intentionally blank

Attachment C2: Annex — Oil and Natural Gas Subsector Pandemic Influenza Guideline

ANNEX: Oil and Natural Gas Subsector Pandemic Influenza Guideline

Purpose: This Sector-specific guideline is an annex to the *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* (*CIKR Pandemic Influenza Guide*) and intends to assist the Oil and Natural Gas (ONG) Sector plan for a catastrophic influenza pandemic. Companies that fail to prepare for such a prolonged catastrophic event may find themselves without the staff, equipment, or supplies necessary to continue providing oil and natural gas to their customers and the nation. For a copy of the complete CIKR Pandemic Influenza Guide, please see www.pandemicflu.gov/plan/pdf/cikrpandemicinfluenzaguide.pdf.

How-to-Use Guidelines: The guideline serves as a non-prescriptive reference for owner-operators and a practical tool that business planners can use to augment and tailor their existing emergency response plans given the unique challenges a pandemic influenza presents. **It is important to integrate your pandemic influenza plan with your existing business continuity and emergency response plans and/or the CIKR Pandemic Influenza Guide's comprehensive framework for pandemic influenza catastrophic planning.** This annex addresses some of the unique challenges the ONG Sector may face during a pandemic influenza, as well as the seven major areas of vulnerability the Sector should assess fully in planning for a pandemic influenza. While not necessarily applicable to all businesses or entities in a given sector, each relevant *Action*, *Supporting Action,* and *Question* in this Guideline can be integrated and managed as a separate checklist item during the planning process.

- **Actions**: These are primary checklist items with numerous related supporting actions and questions to consider.
- **Supporting Actions**: Expanding on the overarching action, these supporting actions offer suggestions for further study.
- **Questions to Consider**: These questions are designed to focus on the main and supporting actions. The questions are not comprehensive; they are designed simply to represent a starting point to stimulate thinking about further actions and options.

Planning Assumptions: Influenza pandemics are unpredictable; it is impossible to forecast the characteristics or severity of a pandemic flu virus accurately. However, if a severe influenza pandemic emerges, given today's highly mobile population, outbreaks may occur nearly simultaneously across the country making reallocation of resources more difficult than with other emergencies. Therefore, each sector must evaluate their own dependencies with critical providers of products and or services to maintain an acceptable level of system operation to meet predefined pandemic influenza service level requirements. While an influenza pandemic will likely affect a given community for six to eight weeks, nationally a wave may linger for up to 12 weeks. Thus, even though a community outbreak may have subsided, businesses in those communities that depend on a national supply chain may find themselves without the necessary materials, supplies, and workforce because other communities across the country may still be affected by an outbreak. The guidance, which is based on disease impact assumptions (pandemicflu.gov/plan/pandplan.html) from the Centers for Disease Control and Prevention (CDC), includes the following.

- *Susceptibility to the pandemic influenza virus will be universal.*
- *Once sustained person-to-person transmission begins, the disease will spread rapidly around the globe.*
- *The clinical disease attack rate will likely be 30 percent or higher in the overall population during the pandemic influenza.*

- *Rates of absenteeism will depend on the severity of the influenza pandemic. In a severe pandemic influenza, absenteeism attributable to illness, the need to care for ill family members and fear of infection may reach 40 percent during the peak weeks of a community outbreak.*
- *Epidemics will last 6-8 weeks in affected communities.*
- *Multiple waves (periods where community outbreaks strike across the country) will likely occur with each lasting 2-3 months.*

For detailed information on the complete set of planning assumptions and the pandemic influenza context, see Section 3 of the *CIKR Pandemic Influenza Guide* and the other Federal guidance at www.pandemicflu.gov.

ESSENTIAL SERVICES AND FUNCTIONS

Industries in all sectors of the American economy will experience influenza pandemic impacts - the ONG Sector is no exception. Effective coordination with public safety officials and community leaders will facilitate the integration of ONG businesses into community emergency operations plans. The essential services and functions of the petroleum portion of the ONG Sector include the production, transportation and storage of crude oil and natural gas; the processing of crude oil into petroleum products; the transmission, storage and wholesale retail distribution of petroleum products; and control systems to coordinate storage and transportation. The essential services and functions of the natural gas portion of the ONG Sector include the production, processing, transportation, distribution, and storage of natural gas; liquefied natural gas facilities; and gas control systems. All CIKR sectors depend on fuel, and the Chemical Sector is dependent on ONG as feedstock. Any interruption in the supply of petroleum or natural gas would do significant damage to the U.S. economy and the American people.

ACTION **Identify and assess your company's essential products, services, and functions.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify essential services that must keep operating and identify the critical functions needed to support those services (e.g., control rooms, plant operations, key systems support, scheduling, etc).	• What functions and processes must you sustain to produce, distribute, and maintain critical services and functions? • Who are your critical customers? Can you prioritize essential services and functions specifically to serve critical customers (e.g., hospitals)? If so, can you deliver fuel to them independently of your other customers? • Have you communicated with your service providers, suppliers, government entities, health care providers, and critical customers about the need to jointly plan for a pandemic influenza? • Have you revised your incident management capabilities to address a pandemic influenza threat? • Have you devised plans to accommodate for the resulting impact of suspending or restaging (e.g. split shifts) certain operations? • Have you established alternatives to limit cash transactions with the public? If outside service provides for bill payment or collections, are there plans for continuity of service? • Have you communicated with your financial institutions on how they will support your continued need and ability to make appropriate fund transfers should the pandemic influenza affect usual mechanisms for funding suppliers and paying employees?
❑	Identify services and functions (e.g., meter reading, training, etc) that you can suspend.	
❑	Prioritize essential services and functions given their value to your critical customers and the community.	
❑	To ensure continuity of products and services, assess remote connectivity and accessibility options for workers.	

ESSENTIAL SYSTEMS AND EQUIPMENT

Unlike other disasters, an influenza pandemic will not physically damage infrastructure. However, emergency planners should assess the affect absenteeism could have on essential equipment operations. In addition, a pandemic influenza's impact on the supply chain (i.e., "just-in-time" delivery, warehousing, and logistics) could significantly impact your ability to procure replacement parts and supplies, or to conduct routine maintenance. Planners should have contingency plans that address the lack of parts and supplies for operating essential equipment and assets. Essential systems and equipment include, but are not limited to: wellheads, gas and oil separation plants, oil/gas dehydration units, oil/gas sweetening units, compressor stations, emulsion breaker units, water treatment units, pipelines, port facilities, unloading facilities, storage facilities, refineries, ocean tankers, barges, trucks, railroad tank cars, storage fields, tank farms, natural gas processing plants, liquefied natural gas (LNG) facilities, natural gas control systems, gas market centers, and information systems/SCADA systems.

ACTION **Review systems and equipment critical to support each essential function.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify equipment that must operate continuously and/or at key periods to sustain essential functions and processes.	• How will you maintain and repair essential equipment given potential supply chain issues? • Can typical processes be modified temporarily to sustain essential systems and equipment?
❑	Identify and prioritize safety and security requirements for maintaining essential equipment and assets.	• Is your equipment clearly mapped and marked so it can be located in case of emergency repair or replacement by non-regular staff? • Do you have pre-established contracts with multiple equipment vendors for emergency replacement and repair during an influenza pandemic?
❑	Review primary and supporting components of critical equipment to identify potential critical system failures and possible cascading consequences.	• Has a full assessment been conducted for all critical systems to identify potential failures based on the pandemic influenza planning assumptions? • How will concern about public contact and disease transmission affect demand for oil products, LNG, propane, and natural gas? Will it affect your essential systems and equipment?
❑	Consider how each action relates to those actions you have already developed in your organization's contingency plans to address other emergencies.	• Have standard operating and emergency procedures (e.g. entering properties to discontinue or establish service) been developed for all essential processes and equipment? If so, have they been distributed broadly to managers and staff?
❑	Consider a plan with regulators to suspend or extend non-essential compliance deadlines	• When assessing potential critical system failures, what are the possible primary/supporting system and equipment challenges (e.g., maintenance technician availability; standard replacement and repair part accessibility; operation of SCADA and information systems)?

ACTION	Prepare to sustain essential systems and equipment for a wave lasting up to three months.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Prioritize the options available to address demands on your essential resources.	• What is the frequency for routine maintenance on essential primary/secondary assets and equipment? How critical is it to perform on this schedule? How easily can scheduled maintenance be deferred or accelerated on short notice? • Is your regular routine maintenance on your essential equipment up-to-date, and how much routine maintenance is required for this equipment during a pandemic influenza wave? • Is there excess operational capacity for your essential equipment to sustain functions while alternating and reducing demands on specific equipment and workers (e.g., using alternate modes of transport for delivery of oil, LNG, diesel or gasoline)? • Do you have replacements available for all essential equipment either on-site or locally? • Do you have emergency equipment available (e.g., generators) if you lose equipment or its fuel supply? • Do you have updated standard operating procedures for this equipment, and have you changed them to address pandemic influenza conditions (e.g., social distancing strategies)? • Have you considered how you would maintain essential services and functions if another disastrous event (such as a hurricane or ice storm) affected your critical systems and equipment during the pandemic influenza wave? • Without sufficient replacement parts on-site or locally, could a mutual aid pact be formed with other similar facilities to sustain operations? • Are there updated emergency operating plans for all assets/equipment to address an influenza pandemic? Can you incorporate social distancing strategies, disciplined personal hygiene, personal protective equipment (PPE), and equipment decontamination be effectively?
❑	Plan to rely on in-house or available local maintenance and repair/replacement support for 2-3 months during a pandemic influenza wave.	
❑	Assess recurring and preventative maintenance requirements.	
❑	Assess implications if essential assets fail early on during the pandemic influenza outbreak.	
❑	Consider establishing a pandemic influenza mutual aid program among similar small/medium and even large businesses to assist each other with sustaining essential assets.	

ESSENTIAL RAW MATERIALS AND SUPPLIES

While a pandemic influenza "wave" may linger in a community for six to eight weeks, it will likely linger nationally for eight to 12 weeks. The negative impacts on individuals, businesses, and the nation from the illness and disease mitigation strategies will have an impact over a much longer duration than typical disasters. A severe influenza pandemic may disrupt the access to your essential materials and supplies, necessary to function, for up to 12 weeks. Given an increased reliance on "just-in-time" delivery and potential impacts that could shut down the supply chain, you may consider stockpiling food, water, fuel, replacement and maintenance parts, personal protective equipment (PPE) (e.g., masks, gloves) and other infection control supplies (cleaning supplies, tissues, hand sanitizer) on-site or locally.

ACTION **Identify materials and supplies to sustain essential functions and equipment for up to 12 weeks.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify critical materials to ensure distribution capacity.	• How much of which materials/supplies (e.g. chemicals, electricity, fuel) are required to sustain the most essential operations for up to three months? • What can the business afford to stockpile and what must it stockpile? How can these additional extraordinary costs be funded (e.g., retained earnings, special disaster fund, and/or government support)? • Will advance notice of supply-chain disruption be available? Will it be sufficient to switch suppliers or take plants offline? • Can you expand storage capacity temporarily for unused oil/gas to ensure continuity of extraction? • Have you identified the availability and need to stockpile critical systems' replacement and normal maintenance parts in sufficient quantities to sustain operations for three months? • What available supplies might you substitute temporarily for preferred essential ones? • Do you have sufficient PPE and cleaning supplies to ensure high levels of hygiene in common work areas that will be used by personnel required to maintain essential services?
❑	Prioritize essential material and supplies necessary to operate equipment and sustain essential functions.	
❑	Identify options to reduce demand for essential supplies and materials.	
❑	Explore options for expanding stockpiles and close-by storage.	
❑	Assess all internal and external supply-chain support operations and contracts.	

ACTION	Determine the most effective ways to ensure an adequate supply of essential materials.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Assess costs to procure, stock, and/or ensure delivery of essential materials.	• How long is the supply chain from order to delivery for essential supplies (pipes, drill bits)? Have you asked suppliers about changes to delivery timelines during an influenza pandemic?
❑	Identify physical or safety limitations in stocking sufficient critical supplies locally.	• What happens if the supply chain cannot provide critical materials or supplies? How quickly would that affect the business' ability to provide essential services? How will customers, vendors, and government emergency response officials be notified of impacts?
❑	Identify a formal chain of command to ensure someone is available to authorize major emergency procurements.	• How can you provide incentives for essential suppliers and support contractors to become better prepared? For example, can the business collaborate on planning, integrate preparedness training, and stipulate pandemic influenza certification in all supply contracts?
❑	Identify additional security needs for increased high-value material stockpiles.	• To improve availability options, are there pre-established contracts with multiple vendors of essential supplies? Who do the business' vendors rely on for their supply and transport services; are they different or the same providers?
❑	Coordinate with supply-chain vendors, and identify secondary sources for critical supplies.	• Where can additional supplies be stored if on-site capacity is limited? • If you cannot stockpile critical materials or your "just-in-time" supply chain fails, do you have backup plans (e.g., pre-negotiated contracts with new suppliers for priority delivery)? • Are there additional security constraints with off-site storage of supplies? • Have you integrated your planning with your local/regional suppliers to understand what priority level your company has in receiving products and services support?

ESSENTIAL WORKERS

A severe pandemic influenza may cause extended absences for essential workers, which might affect you and your supply chain. During a severe influenza pandemic , workforce absenteeism may range from 25 to 40 percent. Complicating matters, the disease will strike randomly among employees from the boardroom to the mailroom. Implementing disciplined workplace personal hygiene and appropriate social distancing strategies may reduce absentee rates for illness and other related reasons. Organizations may consider stockpiling certain medical (e.g., antiviral medications, see www.pandemicflu.gov/vaccine/medantivirals.html) and non-medical countermeasures (e.g., hand disinfectants, gloves, and masks). Essential workers in the ONG Sector perform functions in the following areas: oil and natural gas extraction, processing (refineries and natural gas plants), petroleum manufacturing, petroleum merchant wholesalers and retailers (e.g. gasoline stations), oil/natural gas pipeline transportation, and natural gas distribution (utilities).

ACTION **Identify the types and numbers of workers critical to sustain essential functions.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify essential workers based on their position/skills necessary to sustain essential functions and equipment.	• Have the worker categories and essential workers been formally identified and communicated to the business' workers and appropriate unions and other organizations? • Are there constraints in employing union contract workers and/or for specific local worker contracts in non-standard ways during an emergency temporarily (e.g., can a skilled maintenance technician temporarily serve as an operator)? • Do you have a cross-training plan to prepare workers for non-standard positions? • Are there differences in your workforce by age and/or family status (e.g., employees with younger children may be affected more by school closures and self-quarantine)? • What are the different workforce challenges for on-site vs. off-site and full vs. part-time contractors to perform critical functions? • What are the potential effects of changes in demand and adjustments in scalable operations on essential worker requirements and numbers? • Have those workers who might not typically be considered "essential" in most disaster scenarios (e.g., janitors) but will become so in an influenza pandemic been assessed? • Are there ways to automate or electronically augment certain essential workforce functions? • What essential operations might you need to maintain temporarily through contract support? • Have you developed plans to modify work schedules to reduce exposure to critical workers?
❑	Define the roles and responsibilities of employees, labor organizations, staff, supervisors, managers, and staff medical personnel during an influenza pandemic.	
❑	Assess impacts from short-term and extended absences by essential workers.	
❑	Assess requirements given differences in operational demands for essential workers	
❑	Assess the options to obtain contractor backup support on essential operations and determine how quickly that can be started.	

ACTION	Identify policies and procedures to ensure a safe workplace.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Emphasize worker/workplace disease control/protection. See: www.pandemicflu.gov/plan/workplaceplanning/index.html.	• Has stockpiling emergency supplies such as food and water been considered for workers who may be retained at the worksite (e.g., control or emergency operations centers) for extended shifts/periods? • What are your plans to enhance worksite cleaning procedures (e.g. increase frequency of routine cleaning of high risk, high traffic areas)? • How will you fund costs associated with stocking worker protection items such as masks, cleaning materials, and, with appropriate medical oversight and support, antivirals? • If anticipated for use, have worker preparedness tasks such as mask and respirator training and fit testing been reviewed and incorporated in the plans based on OSHA requirements (www.osha.gov/Publications/influenza_pandemic.html)? • What impact will requirements for maintaining social distancing, equipment decontamination and worker personal protection have on normal and emergency operations and services for your business (e.g. delay inside building meter reading by LDCs)? • Has closing non-critical common areas, such as break and lunch rooms, and ensuring that shifts do not commingle during shift changes been considered in the plans? • Do you need to update your security plan to ensure the security of your workplace from potential incursion, and protect the transfer of assets?
❑	Determine the types of PPE that may be best for various worker types and worksites. For information on suggested PPE use, see: www.osha.gov/Publications/influenza_pandemic.html.	
❑	Develop protocol (i.e., seek medical attention, avoid workplace, notify supervisor) for employees to follow if they contract the virus, show symptoms, or have ill family members.	
❑	Consider screening employees and visitors at the entrances to your critical facilities.	
❑	Consider limiting workplace access to visitors and other non-essential workers.	

ACTION	Identify policies and procedures to protect and sustain workers during an influenza pandemic	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Reduce demands on essential workers.	• Are there practical temporary options that can be exploited to increase worker availability (e.g., extending shifts to 12 hours, adding overtime, and using other non-essential workers)?
❑	Temporarily augment essential worker ranks.	• Could less essential staff work from home to reduce disease transmission at the workplace?
❑	Consider plans to increase the number of employees who work off-site (i.e., home).	• Has the need for and conditions requiring more extreme measures, such as sequestering repair technicians, or scheduling and dispatch workers on-site been considered?
❑	Develop protocols (i.e., seek medical attention, stay away from work, notify supervisor) for employees to follow if they contract virus, show symptoms, or have ill family members.	• Are your telecommunications and information technology infrastructure capable of shifting calls, data and other services off-site? • Can technicians who largely work alone (e.g., measurement, corrosion, pipeline, etc) get their work assignments without coming to the area plant or office? • What contingency plans are in place to replace helicopter pilots who transport offshore workers to platforms? • Do you have plans to limit exposure to offshore workers who share living quarters during long shifts? • Have wholesale and retail station protocols been developed to encourage social distancing from customers while maintaining adequate service? • Can inside work/maintenance by local distribution companies (LDC's) that requires contact with residents or business customers be delayed until the threat is reduced? Have procedures been developed to protect workers who must enter a residence for emergency response purposes (e.g., leak) in situations where an ill person is in the home? • Will the appropriate regulatory authority allow continued "estimation" of meter reading during pandemic influenza conditions?

ACTION	Identify Human Resource (HR) protective actions and policies to sustain essential workforce.	
✓	**SUPPORTING ACTIONS**	**QUESTIONS TO CONSIDER**
❑	Assess standard HR policies and procedures.	• Have you adapted existing and/or developed new sick leave policies to support ill workers and their ill family members (www.pandemicflu.gov/plan/community/commitigation.html)? • Have you met with union leaders to discuss possibly implementing new temporary policies? • Have you communicated with workers and their families about potential HR policy changes? • Have you identified possible actions to help reduce potential abuse of the leave policies you have adapted to account for the possible extended absences by employees? • Have you identified the legal ramifications of employing emergency HR policies (e.g., costs associated with leave policies)? • Has your company considered using professional health authorities to discuss with essential staff their understanding and willingness to receive antiviral medications and/or vaccines? • Have you consulted with health authorities to understand confidentiality policy issues in working with employees who may or have been potentially been exposed? • Have you developed/updated workforce deployment policies regarding teams and crews working together and potential need to keep employees separated? • Have you developed a staff travel policy (for work and non-work related travel), including possible provisions for quarantine after returning from an infected area? • Have you considered relevant Federal, State, or local laws (e.g., FMLA www.dol.gov/esa/whd/fmla/) that govern extended leave for employees?
❑	Develop additional HR policies specific to pandemic influenza response.	
❑	Identify likely legal considerations that may arise from these new HR actions.	
❑	Develop plans and procedures that provide support and assistance to employees' families.	
❑	Provide regular communication to all staff on the latest health advisories and recommendations regarding the influenza pandemic.	

ESSENTIAL INTERDEPENDENCIES

When a pandemic influenza strikes, it will affect all sectors of society. Preparedness and response requires a coordinated national response, including Federal, State, and local governments and most importantly the private sector. To facilitate a swift pandemic influenza response and recovery, the ONG Sector, and the businesses therein, must identify and sustain its essential interdependencies within and across sectors. The nation's critical infrastructure relies on the ONG Sector for fuel. Conversely, the ONG Sector depends on the Transportation, Banking and Finance, and Communications sectors, among others, to sustain its essential services and functions. The interdependent nature of the Sector presents challenges and opportunities for coordinating public and private sector preparedness activities.

ACTION **Identify interdependent relationships and take actions to sustain this support.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify and assess, as needed, sector and external cross-sector essential service support requirements.	• Within the ONG Sector and other sectors (e.g., Transportation, Communications, Finance), which entities do you depend on most to sustain its essential operations, and vice versa? • How are your raw materials and supplies delivered to you, and will these transportation systems continue a reliable supply of materials during an influenza pandemic?
❑	Identify and assess, as needed, the viability of the various modes of transportation (e.g. rail, barge, trucks) used to deliver raw materials and finished products.	• How are your raw materials and supplies delivered to you, and will these transportation systems continue a reliable supply of materials during an influenza pandemic?
❑	Identify and assess, as needed, the capability of communication channels to function under stress of pandemic influenza environment.	• What steps have you taken to ensure continuity of water and electrical power for your essential services? • If communications networks fail or become unreliable or slow, how will you maintain contact with other suppliers, public sector partners, your customers or other essential parties?
❑	Develop joint operational plans with key service providers, suppliers and customers in the public and private sectors.	• If IT networks are impaired, will monitoring of pipeline integrity be compromised?
❑	Assess capability of mutual aid and assistance networks to reduce vulnerabilities.	• What safety or security requirements will pandemic influenza necessitate and how should you coordinate with public safety officials (e.g., local police, fire departments) and local government officials? • Are there payment collection alternatives if a influenza pandemic disrupts typical payment options (e.g., electronic payment instead of cash)?

	(Cont.) • Are the organization's pandemic influenza plans integrated with other key sector and cross-sector business continuity plans? • Does the organization participate with other security partners in public and private pandemic influenza planning and response training exercises? • Has the LDC integrated its plan with the local government's pandemic influenza response plan in relation to PPE, vaccine distribution, and other local health department planned actions? • How can the LDC's and municipal governments coordinate their planning efforts to ensure a reliable supply of products and services?

REGULATORY ISSUES

In response to an influenza pandemic, the government may provide direct support in the form of vaccines, antiviral medications, and personal protection supplies for essential workers; priority and clearances for a business' supply deliveries; on-site public safety and physical security augmentation. Indirect support may come from governmental relief such as waivers for key regulatory issues specific to a sector. However, companies should not count on possible regulatory relief and/or waivers in their pandemic influenza planning. Early discussions with regulatory officials can best identify issues needing to be addressed before an influenza pandemic.

ACTION **Identify Federal/State/local regulatory regulations that may affect your operations.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Identify regulations that, if temporarily modified, would reduce impacts on critical functions, resources, and workers.	• Are there direct/indirect impacts on business operations that should be addressed, such as enacting temporary safety policies, and enhancing enforcement of existing regulations? • What impacts could result from government response actions and cross-jurisdictional differences in response (e.g., quarantine, widespread or localized travel restrictions)? • Are there temporary regulatory waivers to consider in sustaining essential operations (e.g., extended hours of service, adjusting routine safety inspection schedules, extending compliance deadlines, OQ regulation by DOT)? • What temporary government actions (e.g., regulatory relief, financial or material assistance, or information) may help with continuity and delivery of essential services and functions? • Have you coordinated with federal, local and State officials to raise awareness of possible regulatory relief and/or waivers that may arise during an influenza pandemic? • Are there potential temporary worker and workforce regulatory challenges specific to pandemic influenza that should be considered?
❑	Identify direct/indirect government support options you may need to remain operational.	
❑	Coordinate possible direct and indirect support and specific regulatory constraints and relief options with your appropriate Federal/State/local officials and trade associations.	
❑	Communicate potential relief actions in advance to workers, supporting entities, insurers, and customers.	

IMPACTS FROM COMMUNITY DISEASE MITIGATION STRATEGIES

To reduce pandemic influenza impacts, Federal, State, and local governments, as well as private entities, may implement strategies, including voluntary isolation; voluntary home quarantine; school closures; and community and workplace social distancing. The public health and social distancing strategies may ultimately contain the disease and reduce the risk of infection and death, but they may generate significant costs for businesses. For more information on possible community mitigation strategies, see www.pandemicflu.gov/plan/community/commitigation.html, particularly Appendix 4, and Section 3 of the *CIKR Pandemic Influenza Guide.*

ACTION **Identify effects from mitigation strategies; take actions to reduce negative impacts.**

✓	SUPPORTING ACTIONS	QUESTIONS TO CONSIDER
❑	Calculate effects of Centers for Disease Control's Community Mitigation Strategies (www.pandemicflu.gov/plan/community/commitigation.html) on your company.	• What effects will the strategies have on worker absentee rates (e.g., how will it affect your workers if schools/childcare facilities close for weeks at a time)? • What are the costs associated with expanding your sick leave policies? • How can you survey employees to identify who may need to stay home, telework, or work an alternate schedule to care for children because they are dismissed from school/childcare? • What workplace social distancing measures can you implement (e.g., work-at-home options, split working/meal shifts, remote monitoring, reduced travel, and increased use videoconferencing and teleconferencing)? • Have you met with your local leaders on the timing of measures, alerts, and implementation they are considering for the community at-large as well as potentially for your business, and on the complementary triggers for your operational response? • What are the demand changes to your company when schools and/or businesses close? • Do you have plans and procedures to provide support and assistance to employee families? • Have you compiled a list of employee contact numbers and email addresses to ensure communications during the pandemic influenza? • Has your organization established call-in numbers where employees can uniformly receive updates from management on the current situation?
❑	Consider the need to separate the workforce, establish independent locations, and/or preserve a clean work site.	
❑	Determine the strategies that your State/community may/can employ.	
❑	Discuss with workers the potential impacts from strategies.	
❑	Familiarize yourself with your community's trigger points and the CDC's Pandemic Influenza Severity Index to determine the timing and use of mitigation interventions. For more information, see: www.pandemicflu.gov/plan/community/commitigation.html#IV.	

		(Cont.) • Have you worked with local public health regarding the availability of antivirals or vaccines for staff members who perform critical functions? • Have you considered contracting with a Pharmaceuticals Distribution Manager (PDM) to help manage the legal and logistical aspects of procuring, storing and distributing any PPE, hygienic products or vaccines that your organization secures? • In the event of travel restrictions, have your critical facilities (e.g., refineries, storage tanks) and workers been issued travel authority to ensure continuity of operations?

For more useful pandemic influenza preparedness information, including a PDF copy of the complete *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources*, visit www.pandemicflu.gov or email your questions to dhspandemic@dhs.gov.

This page intentionally blank

Attachment C3: WHO Pandemic Phases and the Federal Government Response Stages

Pandemic Phases

The six phases listed below are based on information developed by the World Health Organization (WHO). Pandemic response plans should be coordinated first with the appropriate local, State, provincial, and Federal Government agencies. In the absence of clear guidance, these six phases provide a useful planning framework for businesses.

<table>
<tr><th colspan="2">WHO Phases</th><th colspan="2">Federal Government Response Stages</th></tr>
<tr><td colspan="4">INTER-PANDEMIC PERIOD</td></tr>
<tr><td>1</td><td>No new influenza virus subtypes have been detected in humans. An influenza virus subtype that has caused a human infection may be present in animals. If present in animals, the risk of human disease is considered to be low.</td><td rowspan="2">0</td><td rowspan="2">New domestic animal outbreak in at-risk country</td></tr>
<tr><td>2</td><td>No new influenza virus subtypes have been detected in humans. However, a circulating animal influenza subtype poses a substantial risk of human disease.</td></tr>
<tr><td colspan="4">PANDEMIC ALERT PERIOD</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Human infection(s) with a new subtype, but no human-to-human spread, or at most rare instances of spread to a close contact.</td><td>0</td><td>New domestic animal outbreak in at-risk country</td></tr>
<tr><td>1</td><td>Suspected human outbreak overseas</td></tr>
<tr><td>4</td><td>Small cluster(s) with limited human-to-human transmission but spread is highly localized, suggesting that the virus is not well adapted to humans.</td><td rowspan="2">2</td><td rowspan="2">Confirmed human outbreak overseas</td></tr>
<tr><td>5</td><td>Larger cluster(s) but human-to-human spread still localized, suggesting that the virus is becoming increasingly better adapted to humans, but may not yet be fully transmissible (substantial pandemic risk).</td></tr>
<tr><td colspan="4">PANDEMIC PERIOD</td></tr>
<tr><td rowspan="4">6</td><td rowspan="4">Pandemic phase: increased and sustained transmission in general population.</td><td>3</td><td>Widespread human outbreaks in multiple locations overseas</td></tr>
<tr><td>4</td><td>First human case in North America</td></tr>
<tr><td>5</td><td>Spread throughout United States</td></tr>
<tr><td>6</td><td>Recovery and preparation for subsequent waves</td></tr>
</table>

Oil and Natural Gas Sector
Influenza Pandemic

Planning, Preparation and Response Reference Guide

This page intentionally blank

Attachment D: State, Local, and Territorial Initiatives for the 2008 Sector CIKR Protection Annual Report for the Energy Sector

The organizations described here have made a significant effort toward achieving the goals and objectives of the Energy SSP. They have sought to assure that critical energy infrastructures are appropriately protected, that investments are made to enhance resiliency, and that State and local governments are prepared to quickly and effectively respond to energy disruptions, supporting and complementing the private sector's response.

D.1.1 National Governors Association (NGA) Center for Best Practices

Founded in 1908, the NGA is the collective voice of the Nation's governors. Its Center for Best Practices develops innovative solutions to today's most pressing public policy challenges, and it is the only R&D firm that directly serves the Nation's governors. The Center's Homeland Security and Technology Division informs States about effective practices in homeland security policy and implementation, addressing bioterrorism, CIP, energy assurance, information sharing, intelligence and emergency management, and government use of information technology. In June 2006, the NGA also formed the Governors Homeland Security Advisors Council to provide an organizational structure in which homeland security directors from each State and Territory could discuss homeland security issues, share information and expertise, and inform governors about issues that could affect the implementation of homeland security policies in the States.

Over the last year, the NGA Center undertook or participated in a number of activities designed to support the security of the U.S. Energy Sector and enhance a national energy assurance strategy. Those activities included the following:

- *Increasing the awareness of governors and their policy staffs about energy assurance challenges and priorities,* by providing direct technical assistance to their offices and by sharing effective strategies and security practices from around the Nation through weekly newsletters, issue briefs, and other publications.

- *Building and improving professional relationships among State homeland security officials, State energy offices, and private industry,* by identifying opportunities for the officials to participate in and make presentations at energy industry conferences, workshops, and other forums, including NASEO's February 2008 Winter Conference in Washington, D.C.

- *Raising the awareness within the energy industry and among State energy officials of the implications that a variety of threats, including the threat of pandemic influenza, could have on the Energy Sector.* The NGA Center included energy industry representatives in a series of pandemic preparedness workshops held throughout 2007 to examine the implications that a severe influenza pandemic would have in a variety of sectors. It also developed recommendations for States to help them address sector-specific pandemic

planning requirements. Representatives included those from ExxonMobil at the Region VI Workshop in New Orleans in June 2007 and from Southern Company at the Region IV Workshop in Atlanta in December 2007.

D.1.2 National Association of Regulator Utility Commissioners (NARUC)

NARUC is an association representing the State public service commissioners who regulate essential utility services — such as electricity, gas, telecommunications, water, and transportation — in 50 States, the District of Columbia, Puerto Rico, and the Virgin Islands. As regulators, the members are charged with protecting the public and ensuring that rates charged by regulated utilities are fair, just, and reasonable. Established in 2002, NARUC's Critical Infrastructure Committee represents 18 States and gives State regulators a forum to analyze solutions to utility infrastructure security and delivery problems and concerns. The committee also gives State regulators opportunities to share effective security practices and collaborate among themselves and with their Federal counterparts.

NARUC has always recognized the importance of CIP. In response to the 9/11 attacks, NARUC created the Ad Hoc Committee on Critical Infrastructure, which was promoted to a full standing committee in 2007. This new Committee on Critical Infrastructure illustrates NARUC's commitment to continuously addressing critical infrastructure issues within the jurisdiction of its members. While this change is internal, it also reflects the larger role that NARUC has played over the past two years in developing CIKR policies and programs at the national level. Currently, NARUC sits on the GCCs in the Energy, Communications, and Water Sectors.

NARUC has worked to raise the awareness of other parties of the role that utility commissions play in infrastructure protection and the awareness of its own members of CI issues. NARUC has also been responsive to other CIP concerns, including pandemic preparedness and protection in interdependent sectors, such as Communications Sector and Water Sector. NARUC passed a resolution encouraging State commissions to create continuity-of-operations plans in the event of a pandemic outbreak, and it urged commissions to work with the utilities within their jurisdictions to develop continuity-of-operations plans too. NARUC also developed a fact sheet on pandemic preparedness for commissions, providing them with links to informational resources from DHS and HHS. Providing NARUC members with information on NIMS and National Response Plan (NRP) training was also a project that NARUC took on in 2007. The chair of NARUC's Committee on Critical Infrastructure wrote a letter to all NARUC members with information on why and how commissioners and staff should partake in NIMS and NRP training.

Over the past two years, NARUC developed and consistently updated a training curriculum for commissioners and commission staff to address State CIP needs. This curriculum was used in five training workshops for NARUC members. The workshops took place at two regional meetings across the country in 2006 and at three in 2007. Over the course of the five workshops, NARUC trained a total of 120 commissioners and commission staff from 44 States, 88 of whom were trained in 2007.

In addition, NARUC held a series of "train the trainers" sessions to more intimately acquaint commissioners and commission staff with the material included in the training curriculum: They involved:

- A series of 12 conference calls to develop the curriculum for the original training session and to incorporate refinements between training sessions.

- Two Webcast training sessions for small but geographically diverse groups. The first Webcast was held on November 11, 2006, and the second was on February 2, 2007.

The "train the trainers" sessions provided 20 commissioners and commission staff members from States across the Nation with the capability to train commission colleagues on the material contained in the CIP curriculum. NARUC staff worked with members of the NARUC Committee on Critical Infrastructure to determine what topics would be covered in the training. Topics addressed included these:

- The role of commissions in CIP.
- Emergency preparedness and energy assurance.
- Interdependencies.
- Regional coordination.
- Cost recovery.
- Protecting sensitive information.

D.1.2.1 Peer-to-Peer Exchange

State practitioners who are experts in developing and implementing State CIP policies and procedures have been working with their colleagues in other States to provide peer-to-peer technical assistance on CIP. The purpose of this task is for States to develop or update policies and procedures related to:

- State cost-recovery policies and procedures.
- State and Federal sharing of confidential information.
- State procedures related to more efficient interstate and intrastate communications between officials responsible for CIP.

Two in-person "assistance missions" to States took place in 2006 and proved to be effective, so two more were held in 2007. The first occurred in June 2007 in New York City. Here Texas, Colorado, and Ohio were involved in providing technical assistance focused on interdependencies (particularly with regard to Water Sector and Communications Sector issues), sharing information, cost recovery, and in-state and cross-state coordination. At this meeting, issues and priorities were sketched out and initial "homework" questions were identified. State utility commission representatives committed to investigating their commission's policies with regard to continuity-of-operations planning, CIKR asset management, and staff training opportunities.

The second technical assistance session was held in Anaheim, California, in November 2007. This session included Alabama, Missouri, New Jersey, California, Hawaii, and Michigan in addition to Texas, Colorado, and Ohio. It focused on a full range of preparedness issues across the electricity, gas, water, telecommunications, and transportation infrastructures. Before the meeting, several States had submitted written responses to "homework" questions, and each State agreed to investigate key policies and strategies that might be useful in the State.

In addition to these nine initial State leaders, a "second flight" of eight more States has received technical assistance to prepare for sessions in 2008. Also, in addition to these eight, more States that were unable to participate at the in-person meetings, including Maine and New Hampshire, have submitted action items and responses to the questions. The District of Columbia, Oklahoma, and South Carolina are also beginning to work with State assistance partners to develop an action plan for adopting effective CIP security practices and policies at their State PUCs.

D.1.2.2 Information Protection and Cost Recovery Research

NARUC engaged experts to develop research that would help State regulators become fully involved in Federal and State efforts to establish consistent critical infrastructure information programs. Its report, entitled *Information Sharing in Regulated Critical Infrastructures,* concludes that State public service commissions must be explicitly designated as authorized users of critical infrastructure information, and it encourages the adoption of common terms and methodologies to improve communication among federal and State agencies. The report was developed with input from the States and from DHS's PCII Program. The report proposes that State public service commissions be authorized users of PCII because of their crucial role in overseeing the utility sector. The report also makes a number of recommendations for the use of PCII, including a consistent definition and consistent use of the term "critical infrastructure information" (CII) and the establishment of a confidential hearing process for CII matters. More than 300 copies of this report have been disseminated to State regulators and legislators, among other State decisionmakers.

Participants in Energy Assurance Planning Projects

- *Alabama*
- *California*
- *Colorado*
- *District of Columbia*
- *Indiana*
- *Iowa*
- *Missouri*
- *Nebraska*
- *Nevada*
- *Massachusetts*
- *Oregon*
- *Washington*

D.1.3 National Association of State Energy Officials (NASEO)

NASEO is the only nonprofit organization that represents governor-designated energy officials from each State and Territory. It was created to improve the effectiveness and quality of State energy programs and policies, provide policy input and analysis, share successes among the States, and serve as a repository of information on energy issues of concern to the States and their citizens.

Since 2005, NASEO, with support from DOE's Office of Electricity Delivery and Energy Reliability, has provided funds to

12 State and Territory energy offices in the form of technical assistance grants to support energy assurance resiliency planning and organizational coordination. The grants have helped State and Territory energy offices to update and revise their energy emergency plans on the basis of NASEO's State energy assurance guidelines, incorporate State elements of the NIPP and Energy SSP, and/or increase interorganizational planning and coordination in order to improve energy emergency response and preparedness and protect critical energy infrastructure through enhanced resiliency. By May 2008, California, Colorado, Indiana, Nebraska, Nevada, Oregon, and Washington were to have completed the work to be done under these technical assistance grants awarded in 2007. A third round of grants was awarded in May 2008 to the U.S. Virgin Islands, Oregon, and the District of Columbia to undertake energy assurance work in the coming year.

On October 9, 2007, NASEO, in conjunction with DOE's Office of Electricity Delivery and Energy Reliability and EIA, hosted the 2007/2008 Winter Fuels Outlook Conference at the National Press Club in Washington, D.C. The conference was presented on October 9. About 115 attendees participated in the conference, which was covered by several reporters and news media representatives such as Bloomberg News, Reuters, and the *Wall Street Journal.* More than a dozen staff members from various State and Territory energy offices attended the conference, as well as staff from Washington, D.C.-based trade associations, utility companies, energy service companies, investment firms, and Federal agencies such as DHS, USCG, Congressional Research Services, and the Library of Congress.

Finally, NASEO hosted its 2008 Winter Conference at the Omni Shoreham Hotel in Washington, D.C., on February 3–5, 2008. The conference, which attracted about 135 attendees from 33 State and Territory energy offices, included a plenary session entitled, "Critical Energy Infrastructure and Energy Emergency Responses in States." The session featured speakers from DOE's Office of Electricity Delivery and Energy Reliability, the New Jersey Office of Homeland Security, and the City and County of Denver, who discussed the need for Federal, State, and local cooperation in ensuring the success of energy assurance and reliability activities within the States.

D.1.4 National Conference of State Legislatures (NCSL)

NCSL is a bipartisan organization that serves the legislators and staffs of the Nation's 50 States and its commonwealths and territories. NCSL provides research, technical assistance, and opportunities for policymakers to exchange ideas on the most pressing State issues. NCSL has 11 standing committees. With more than 600 members of State legislatures, the Agriculture, Environment and Energy Committee has jurisdiction over energy production, natural disaster mitigation, and pipeline safety. The Homeland Security and Emergency Preparedness Task Force, which is composed of 30 legislators and legislative staff, shares information on the relevant informational, financial, and physical resources of State and local governments and the Federal Government in an effort to maximize the contributions that each level of government can provide to improve homeland security. In addition, this task force helps legislatures share their expertise and provide advice on issues of public safety, homeland security, emergency preparedness, and public health in order to protect our democratic institutions and way of life.

NCSL's Homeland Security and Emergency Preparedness Task Force held two meetings in the past year that focused on CIP and information security. On November 27 and 28, 2007, legislators and legislative staff from 12 States convened to hear presentations on the PCII, NIPP, resiliency and distributed resources, and cost recovery and information security issues. The presentations on the following day covered the NRF, SAFECOM, the National Guard, and national emergencies. NARUC also assisted with and supported this effort. This task force has been in existence since September 11, 2001, and it usually focused on response issues; a link has now been made between this group and CIP and information security issues. The group members felt that they learned a lot at the November 2007 meeting and requested a follow-up meeting in April 2008. This was held on April 23 and 24.

The April task force meeting focused on critical infrastructure and interdependencies. Legislators and legislative staff members from 12 States attended. The meeting covered communication networks and water infrastructure interdependencies and an update on the NRF.
NCSL published a 30-page CIP primer for State officials (specifically legislators and legislative staff). The primer defines CIP and focuses on three main components of CIP: cost recovery of utility investments, information disclosure, and distributed energy resources. NARUC also assisted with this effort, drawing on the work it did in these areas. The primer then provides State policy options to protect critical infrastructure. Each State house library received a copy, and the primer is available on line through the NCSL bookstore. Electronic versions are also available through the NCSL Energy Program Web page. Copies are distributed at NCSL annual meetings (100 were distributed to legislators, legislative staff, and industry representatives at NCSL's Spring Forum on April 25, 2008, in Washington, D.C.).

D.1.5 Local Governments: Public Technology Institute (PTI)

Established in 1971, PTI works with a core network of leading local government officials in cities and counties to identify opportunities to conduct technology research, share effective security practices, offer consultancies and pilot demonstrations, promote technology development initiatives, and develop educational programming. Officials from PTI member-governments participate in councils and forums that address specific technological areas. Through its partnerships with industry, Federal agencies, and other governmental organizations, PTI shares the results of its activities and the expertise of its members with a broader audience of the more than 30,000 U.S. cities and counties. PTI continues to enjoy a close relationship with the National League of Cities, National Association of Counties, and International City/County Management Association. PTI has a Public Safety Technology and Homeland Security Council that addresses the challenging issues facing cities and counties as they seek to improve their delivery of services through the deployment of new public safety technologies.

PTI has taken a lead role in working with local governments to support energy assurance efforts and implement the Energy SSP. Over the last 12 months, PTI has accomplished the following:

- Presented the first draft of the *Local Government Energy Assurance Guidelines* and Energy Hardening Assessment Tool to the 135-member Sustainability Council for its

review and comments during the PTI Annual Technology Leadership Conference on May 6–8, 2008, in Miami, Florida.

- Developed and completed (in March 2008) an energy supply checklist for energy assurance planning to be used by local governments. This checklist will become part of the *Local Government Energy Assurance Guidelines.*

- Presented the PTI project to the Colorado Intergovernmental Critical Facility Committee (10 members) in December 2007.

- Finished the first complete draft of the *Local Government Energy Assurance Guidelines* in statement and bullet form. Each aspect of the guidelines will be supported by accompanying materials and forms to help local governments understand and use the guidelines. The intent is to make the guidelines very user-friendly and adaptable.

- In October and November 2007, held a kick-off meeting for the Denver pilot with Denver Public Works – Utilities, Denver Environmental Health, Denver Water, and Xcel Energy. A complete pilot work plan was developed for the next year. PTI successfully included the local government methodology for determining critical facility energy assurance into Denver's Emergency Support Function 12 (ESF-12) multiyear work plan.

Two examples of the very wide range of activities that have taken place at the State and local levels follow on the next two pages.

2007 DOE/NASEO Technical Assistance Grant
Fall Energy Emergency Preparedness Activities — Washington State

Keeping Partnerships Alive for Energy Assurance

The State of Washington has 63 electric utilities, eight natural gas transmission and distribution companies, five oil refiners, and additional marketers, distributors, and jobbers. Maintaining capability to work with any and all of them during energy emergencies and supply shortages is difficult. Companies, employees, and telephone numbers change.

Following a severe 2006 windstorm that resulted in outages for about 40 percent of Washington's citizens, Washington's energy office, officially known as the Department of Community, Trade, and Economic Development, Energy Policy Division, proposed a technical assistant grant that would significantly improve the State's capability to respond to energy emergencies in partnership with regional energy companies.

The innovative proposal was to produce a video about the State Energy Emergencies and Security Program, its Energy Assurance Plan, and the partnership concept; hold four energy emergency seminars; and conduct a tabletop exercise where the partnership concept could be tested.

In 2007, Washington faced another severe storm that blacked out most of four counties, flooded tens of thousands of acres, and shut down hundreds of miles of roads including Interstate-5 (closed for three days). The differences in response to the two storms were striking. Utilities assigned top managers to work with the State energy office. Utilities understood the kind of information the State needed and the kind of assistance they could provide. The State was able to dispatch fuel when needed, provide utilities with flaggers to protect workers from traffic, and drop gravel on flooded ground to allow utility trucks to reach downed lines. Utility mangers referred to the video and seminars as tools that helped them understand the State program and what it could do for them.

The video appears to have been a superb idea. The State had sent utilities its 60-page energy assurance plan three months before the 2006 windstorm. It appears that very few even read it. In contrast, at seminars, there were representatives from utilities whose entire emergency response teams had already watched the short video. While the State energy office will continue to hold occasional seminars and exercises, the video is available on the agency Web site at http://www.cted.wa.gov/site/975/default.aspx. The intent is to send all the energy companies in Washington that video link every fall at the beginning of storm season. In addition, the video has already been shown at DOE and NASEO training exercises and conferences, enabling the experiences of one State to be shared with many others.

**Michigan Infrastructure Coordinating Committee (MICC)
and State and Local Coordination with the Energy Sector**

In 2008, Michigan restructured its approach to CIP to better align its efforts with NIPP. MICC serves as a cross-sector coordinating committee with representation from the public and private sector from each of the 18 CIKR Sectors defined in NIPP plus a Schools Sector. The Energy Sector Committee, which had previously existed under the former state CIP Committee, was expanded to more fully encompass all elements of the Energy Sector and now includes representation from electric and gas utilities (large and small), transmission companies, independent power producers, the petroleum industry (including refiners, marketers, and propane dealers), and petroleum product and natural gas pipelines. Staff from the Michigan Public Service Commission and Consumers Energy Company co-chair this committee, with support from the Michigan State Police, Emergency Management, and Homeland Security Divisions. The Energy Committee will be the focal point for the public/private sector partnership in Michigan. The Committee's initial focus is on enhanced information exchange and alert notification, and it is identifying an agenda to direct its efforts in the coming year.

The State of Michigan has also focused on state and local coordination with the energy sector. In 2007, Michigan conducted two workshops for the owner and operators of energy facilities and first responders (local fire, police, and emergency management). This gave first responders a chance to exchange information on safety and security issues related to dealing with an energy facility or energy distribution infrastructure. It also allowed the energy industry to more fully understand the capabilities of the first responder community when dealing with their energy facilities or distribution system.

A workshop held in Michigan's Upper Peninsula focused on experience gained from the Dead River dam failure in 2003. This event caused a release of more than 8 billion gallons of water, and the ensuing flood damaged businesses, roadways, bridges, and private property. The flood waters shut down the only major coal-fired generating plant in the Upper Peninsula, which generated two-thirds of the power used on the Upper Peninsula. This precipitated an energy emergency that lingered for a month as the area's major electric utility worked to keep the lights on. Officials from both the utility and transmission company spoke about how they accomplished this task, how Upper Peninsula emergency responders addressed their actions in dealing with the flood, and how they applied Incident Command.

At the second workshop, there was no focus on a single, dramatic incident like the Dead River flood. Instead, more general topics were a basis of the presentations. Topics such as the interdependencies between energy infrastructures and Incident Command were presented to the attendees. A speaker from one of Michigan's larger utilities discussed its outreach program to first responders. A presentation on general electric and natural gas safety rounded out the program.

Both workshops featured basic safety issues and presented practical information regarding safety around downed power lines and how to safely exit a vehicle that was potentially energized by a fallen line. The state's propane industry addressed the properties of propane gas, how it differed from natural gas, and how to safely contain propane gas leaks.

A total of 166 individuals attended the two sessions. In their evaluations, 80 percent of those who attended said they would be suggesting or making changes at their operations, and 71 percent expressed an interest in attending future workshops. This is just one example of a state and local effort to build the public/private partnership that will allow for a quicker and more effective response that was envisioned in NIPP.

More specific examples of programs and initiatives undertaken by the State and local government groups that directly support the NIPP implementation are included in table D-1. This table summarizes additional activities that have been undertaken by the various groups since the submission of the 2007 annual report.

Table D-1: State and Local Governments' Activities (April 2007–May 2008)

Date	Organizations	Activity
April 24 and 25, 2007	DOE, NARUC, NASEO, NCSL, NGA, and PTI	NASEO and NARUC supported DOE-OE in planning and coordinating the Tabletop Black Water–Southeast Energy–Water Interdependence Exercise held April 24 and 25, 2007, in Decatur, Georgia. The objective of the exercise was to increase participants' understanding of the interdependencies between the Energy Sector and the water supply and wastewater management system.
June 19 and 20, 2007	DOE, NARUC, NASEO, NCSL, NGA, and PTI	NASEO and NARUC were responsible for the logistical planning and coordinating of the Dark Storm: Northeast Energy Assurance Exercise held in Princeton, New Jersey. The exercise attracted more than 90 participants from 11 State and Territory energy offices and public utility commissions in the Northeast and Mid-Atlantic Regions.
June 2007	NARUC, Texas, Colorado, and Ohio	They participated in an in-person assistance mission that focused on interdependencies, particularly with regard to Water Sector and Communications Sector issues, as well as information sharing, cost recovery, and in-state and cross-state coordination.
June 2007	NGA	The NGA Center included representatives of the energy industry in a series of pandemic preparedness workshops held in New Orleans to examine the implications of a severe influenza pandemic in a variety of sectors and developed recommendations for States to address sector-specific pandemic planning requirements.
August 7, 2007	DOE, NARUC, NASEO, NCSL, PTI	DOE's Office of Electricity Delivery and Energy Reliability held a security partner planning meeting involving State and local participating organizations in Hershey, Pennsylvania. During this meeting, FY 2008 priorities were discussed. Progress during the past year and program concepts for the coming years were discussed. Participants identified common areas of interest and potential points of collaboration that have helped guide the work of these groups over the last year.
September 9–12, 2007	NASEO	NASEO hosted the 2007 annual meeting, which included a concurrent session of NASEO's Energy, Data and Security Committee. The session featured a review of NIPP and the Energy SSP and a discussion of the supporting role that State and Territory energy offices play.

Table D-1 (Cont.)

Date	Organizations	Activity
October 9, 2007	NASEO, DOE, and EIA	They hosted the 2007/2008 Winter Fuels Outlook Conference. About 115 attendees participated, including more than a dozen staff members from various State and Territory energy offices as well as staff from utility companies, energy service companies, investment firms, and Federal agencies.
November 2007	NARUC, Alabama, Missouri, New Jersey, California, Colorado, Texas, Ohio, Hawaii, and Michigan	Participated in in-person assistance mission that focused on interdependencies, particularly Water Sector and Communications Sector issues, as well as information sharing, cost recovery, and in-state and cross-state coordination.
November 27, 2007	NCSL	NCSL's Task Force on Homeland Security and Emergency Preparedness held the first of two meetings focusing on CIP and information security. Legislators and staff from 12 States heard presentations on the PCII, NIPP, resiliency and distributed resources, cost recovery and information security issues, and the NRF.
December 2007	NGA	The NGA Center included representatives of the energy industry in a series of pandemic preparedness workshops held in Atlanta to examine the implications of a severe influenza pandemic in a variety of sectors. It developed recommendations for States on how to address sector-specific pandemic planning requirements.
December 13, 2007	NASEO	NASEO hosted a "High Oil Prices and State Responses" conference call that involved 46 attendees from 24 States and featured speakers from the EIA, API, Georgia Environmental Facilities Authority, Massachusetts Division of Energy Resources, and California Energy Commission.
January 31, 2008	NCSL	NCSL hosted the first of three regional conference calls with Midwestern and Western State energy emergency and assurance coordinators. The calls focused on State activities and recent energy and emergency situations and disruptions.
February 3–5, 2008	NASEO	NASEO hosted the 2008 Winter Conference of State energy officials. About 135 attendees from more than 33 State and Territory energy offices participated. It focused on the need for Federal, State, and local cooperation in ensuring the success of energy assurance and reliability activities within the States.
February 29, 2008	NCSL	NCSL hosted the second of three regional conference calls with Midwestern and Western State energy emergency and assurance coordinators. The calls focused on State activities and recent energy and emergency situations and disruptions.
March 2008	PTI	PTI completed an energy supply checklist for energy assurance planning use at the local government level.

Table D-1 (Cont.)

Date	Organizations	Activity
March 20, 2008	NCSL	NCSL hosted the third of three regional conference calls with Midwestern and Western State energy emergency and assurance coordinators. The calls focused on State activities and recent energy and emergency situations and disruptions.
April 22 and 23, 2008	DOE, NARUC, NASEO, NCSL, NGA, and PTI	NCSL, in conjunction with DOE, hosted the Summer Fuels Outlook Conference and Workshop on Building Energy Resiliency into Energy Assurance Planning in Denver, Colorado. The workshop was attended by representatives from the Federal and State governments, select private sector participants, nonprofit organizations, and major municipalities and local governments. State agencies included public utility commissions, energy offices, emergency management agencies, and homeland security advisors and administrators. A total of 76 individuals participated, including representatives from 21 States and two municipalities
April 23 and 24, 2008	NCSL	NCSL's Task Force on Homeland Security and Emergency Preparedness held the second of two meetings focusing on CIP and information security. It covered communication networks, water infrastructure interdependencies, and an update on the NRF.
April 25, 2008	NCSL	NCSL distributed its 30-page CIP primer to State officials, including legislators and legislative staff.
May 6–8, 2008	PTI	PTI held its Annual Technology Leadership Conference. It released the first draft of its *Local Government Energy Assurance Guidelines* and Energy Hardening Assessment Tool to the 125-member Sustainability Council.
May 6, 2008	NASEO	NASEO hosted a second conference call on "High Oil Prices and Short- and Long-Term State Responses." Sixty individuals representing 31 States participated.

Attachment E: Visualization and Modeling Working Group

E.1 Group Progress

The VMWG is a consortium of national laboratories — including Argonne National Laboratory, Los Alamos National Laboratory, National Energy Technology Laboratory, Oak Ridge National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories — and representatives from USACE. Each national laboratory provides modeling capability as directed by the VMWG Playbook. The VMWG, managed and funded by DOE-OE, is responsible for providing geospatial analysis and modeling during energy emergencies. The primary recipient of the information from these efforts is DOE senior management, but the VMWG is also capable of dissemination the data more widely to various government and private sector partners. The VMWG operates under an established Playbook to conduct annual exercises and workshops in an effort to consistently improve its analyses and outreach to external partners, as described below.

E.1.1 Playbook

The Playbook provides guidelines for the VMWG on how to quickly respond to requests for data, analyses, and geographic information system outputs during energy emergencies and exercises. The Playbook outlines the processes to be followed, resources to be used, and roles and responsibilities of each VMWG member, and it provides information on vital operations needed to access and post analyses, including identifying the points of contact on the laboratory team. The response model defined by the Playbook leverages each laboratory partner's modeling capabilities in order to provide sector-specific responses in the form of a forecast of the disruption consequences or a recovery analysis. Defined roles include conducting analyses for all sectors, including electricity, natural gas and petroleum, transportation, demographics, economic impacts, and interdependencies. The VMWG owes much of its success in providing quality products quickly to its clear delineation of responsibilities. The Playbook is a dynamic document that can be augmented to include new Federal agencies as well as energy industry and public sector partners that cooperate with the VMWG. The utility of the document has been thoroughly validated through numerous exercises and through its use for responding to actual events such as Hurricanes Katrina and Rita.

E.1.2 Workshops

The VMWG meets annually to discuss methods for improving internal operations and reaching out to other agencies and interested security partners. Topics covered at these workshops range from lessons learned from past exercises and actual responses, to new tools for improving VMWG response and analysis capabilities, to methods for increasing intersector collaborations. The VMWG national laboratory members rotate the responsibility for hosting workshops. The meetings have grown to include representatives from the energy, healthcare, financial, and other

sectors; Federal agencies such as USACE, HHS, DOD, and the U.S. Department of the Treasury; and State and local governments. The VMWG constantly seeks to collaborate with groups outside the Energy Sector, and this effort is a key factor in the success of these workshops.

E.1.3 Exercises

At least once each year, the VMWG completes an exercise that tests its ability to provide quick analysis of energy emergency scenarios. These exercises help identify measures for improving response capabilities during actual emergencies. The exercises usually culminate in a briefing to representatives from DOE and the Federal agencies and non-public-sector clients that rely on information from the VMWG during these emergencies. These exercises are critical in that they help to ensure that the data and analyses produced by the VMWG are useful. Examples of exercise scenarios include a hydro dam failure in the Southeast United States and the dispersal of anthrax bacteria in various cities. The dam failure exercise required extensive modeling of both the impact on the surrounding population and the impact on the power grid. The anthrax emergency exercise was a joint effort in conjunction with HHS. These exercises are important in that they challenge the VMWG to respond to scenarios that require detailed analyses in a short time period, typically 24 hours.

E.2 National Planning Scenarios

The Homeland Security Council has defined 15 national planning scenarios with the intent of establishing a range of response requirements to facilitate preparedness and planning. Tools and techniques need to be developed to extend these scenarios to energy facilities and to build a cooperative relationship among security partners, energy responders, and the community. The Energy Sector remains committed to the previous suggestions for an exercise or simulation to extend either Scenario Eight (Chlorine Explosion) or Scenario Fifteen (Cyber Attack), as appropriate, to energy facilities.

To build cooperative relationships between security partners and Energy Sector responders, the VMWG helped HHS staff draft an emergency exercise scenario focused on Scenario Three (Aerosol Anthrax Attack),with VMWG inserting a component that could potentially result in significant impacts to relevant energy infrastructures. The scenario was first used in an HHS-sponsored Secretary's Quarterly Readiness Exercise (SQREx) 08-1 (Anthrax) Senior Officials' Tabletop Exercise (TTX).

Subsequent to the HHS SQREx TTX, the scenario was presented to the VMWG in the form of an "Exercise Team Activation," with a comprehensive analysis of Energy Sector impacts being conducted by VMWG Team members. Participating during the exercise were HHS staff members, who served as both HHS subject matter experts and exercise observers.

The success of the joint effort to build cooperation can only be accurately benchmarked after a national emergency in which HHS and DOE would have to proactively work together during response and recovery. However, communication between the agencies was established, and the

contributions of appropriate subject matter experts were recognized, and obstacles and other impediments to HHS/DOE cooperation during an emergency were clearly identified.

E.3 Dependency and Interdependency Analysis

As a result of the current tautness of the petroleum markets, there is the prospect that an emergency in the petroleum subsector could cause U.S. gasoline prices to rise to new record highs. A dependency analysis currently being carried out addresses the degree of dependency of petroleum infrastructure assets on commercial electric power and natural gas. This dependency analysis can be used to determine the consequences to a petroleum asset in the form of either reduced operating rates or a complete shutdown as the result of a disruption of these energy inputs. This information would need to be updated annually, since the degree of the petroleum subsector's dependence on commercial electricity and natural gas can change significantly with time (e.g., due to the construction of cogeneration capacity within a refinery or the addition of a new process unit). Inclusion of such data into the VMWG analysis ensures correct representation of the interdependencies of the petroleum, natural gas, and electric subsectors.

E.4 Modeling/Monitoring Capabilities and Gaps

A concerted effort was made over the last year to provide managers at DOE with as close to a real time status report on the Nation's electricity grid and natural gas infrastructure as possible. The VMWG is developing capabilities to rapidly (on the order of minutes) provide a first-stage assessment of impacts from major disruptions to the infrastructure. As these capabilities are being established, the system is being designed to include such features as readily producible, HTML-formatted reports to support briefing materials for Federal and State emergency responders. The reports are being developed to enable quick visualization of the health of the infrastructure, in order to establish a situational awareness capability within the DOE EOC. The supporting data feeds for this capability are being provided through established agreements with industry, reporting requirements already in place, and existing government-owned or subscription data. The simulation results have been and will continue to be validated though discussions with appropriate industry partners.

Building and maintaining the open-standards-based energy infrastructure data required for these analyses are critical elements of success. The tools that are developed must be able to predict and analyze a wide range of emergency scenarios. To this end, increased collaboration with NISAC, related agencies, and industry partners is needed to validate and access spatial and relational data for various sectors of the energy infrastructure. Relationships between private industry and the government will need to continue to expand. These can establish and validate the credibility of the toolsets and provide opportunities for transferring technologies to the private sector.

There is a continuing need to incorporate sound risk management strategies when assessment capabilities related to the energy subsectors are being developed, so that technologies and resources can be applied to the areas of the infrastructure in which they are most needed.

Real-time assessment capabilities allow users to quickly ascertain the health of the subject infrastructure, so follow-on analysis can be performed to build a more precise understanding of the degree of degradation and speed of subsequent recovery of the systems. This understanding is fundamental for applying sound risk management strategies and will help guide in developing established capabilities further, establishing advanced visualization capabilities in the EOCs, and building resilience within the infrastructure. These tools will then become the foundation for establishing critical nodes with a more global perspective to better understand the dependent and interdependent linkages between private and public sector interests.

Although DOE-OE is not in the business of performing economic analyses, projected energy prices may be considered for inclusion in the VMWG analysis, if only because the changes in these prices are generally the primary way in which the impacts of an incident are distributed beyond the locality in which it occurred. This inclusion is not intended to interfere with the work of traditional economic analysis entities but to help in better defining the scope of potential impacts from a major energy emergency.

E.5 Certification, Verification, and Validation of Modeling and Simulation Results

Representatives from two industry organizations were present at the EOC briefing for the VMWG exercise with HHS. It would be useful to increase the representation of industry groups at these briefings to the extent possible. This would allow for the immediate validation of exercise results and conclusions and assure that the most recent industry information and news (and contacts) were provided as feedback for inclusion in future analyses.

Verification and certification of VMWG modeling and simulation results by industry personnel who work at the potentially affected energy companies would also be advantageous in determining the variety of potential company-specific “workarounds” that might be employed in actual emergency situations. The establishment of working relationships with these persons would facilitate following up on review planning assumptions and defining a process for future coordination.

One issue that has major implications for energy availability is the validation of infrastructure restoration assumptions and models associated with damage from hurricanes and other major weather events. Because information on energy company restoration capabilities and mutual aid agreements is generally unavailable, assumptions made in the VMWG modeling and simulation process should be validated by appropriate industry personnel through post-event reviews.

E.6 Cooperation and Outreach

The VMWG has worked with the Financial Services, Electricity, and Oil and Natural Gas SCCs to share data with participating organizations and establish relationships with private and government partners through annual workshops. To facilitate the sharing of information with such a diverse membership, the VMWG established a Web portal through which response files

are disseminated to members (figure E-1). A server residing and managed at DOE headquarters provides a password-protected working space in which sensitive but unclassified data can be disseminated. As responses are posted, notifications are sent via email to the appropriate members of the portal. Access is managed by a system of member privileges to allow the appropriate level of interaction with the portal. This approach provides exclusive working space for the team members, while the full membership is allowed access only to published reports on the main interface. The importance of having these levels of access is evident during an exercise, when laboratory partners are communicating data and preliminary results. Some users need to view only the final products. The portal has also been extensively used as a reference library of past exercise results and can be used to showcase the modeling and visualization capabilities of the team.

Managers of the site are VMWG members who control the flow of information during an event, which is crucial for producing results in a timely manner. Managers also ensure the posting of results, resolve access problems, and reorganize the files as needed. Currently there are more than 20 government agencies and 15 private organizations represented by about 180 members of the Web portal.

The response documents consist of two components: an executive summary and a full analytical response. While the full response may include more than 50 pages, the executive summary is meant to provide a basis for briefing DOE senior management on the most critical findings in less than 15 minutes and is typically 12 or fewer pages long.

Figure E-1: VMWG Web Portal Welcome Screen

E.7 Emergency Support Function 12 (ESF-12) Emergency Operations Manual

As the lead office for supporting ESF-12 requirements outlined in the NRF, DOE-OE is responsible for responding to energy emergencies of national significance. The emergency operations manual provides instructions and information resources for DOE-OE's EM team and situation report team. It also provides guidelines and instructions for staffing EOCs and offices in the field. In addition, the operations manual provides key guidance on who in the team gathers Energy Sector information, what information they gather, the types of reports that are generated by using that information, and timelines for producing those reports. The guidelines provided can be tailored to event-specific circumstances. The operations manual gives detailed instructions on the roles of OE personnel at DOE headquarters and of personnel dispatched to the field during energy emergencies. It also includes contact information for all team members and instructions on interacting with other agencies. The operations manual is a critical tool in that it provides the EM team with clear guidance on how to respond to energy emergencies in an efficient and timely fashion.

Attachment F: Training

F.1 Overview

F.1.1 Purpose

This attachment reports on the types of training that energy-related trade associations provide to members with regard to security and the prevention of and response to energy emergencies.

F.1.2 Background

DOE and DHS jointly developed the ESSP, which is a NIPP that defines critical infrastructures and identifies who, at all levels of government and the private sector, is responsible for protecting them. Both agencies want to ensure that training on security, threat prevention and response, and energy emergencies is available to members of the Energy Sector. Training could be provided in the form of published materials, classes, Web-based training, or other methods. An assessment is needed to review specific training programs currently offered and to identify gaps that DOE and DHS could help fill.

F.1.3 Approach

For the initial canvassing, the Energy SSP was used to identify associations and organizations that serve the Energy Sector. From this list, security and emergency training programs were identified, principally by looking at the organizations' Web sites and, in some cases, through telephone conversations. This attachment also identifies specific training programs currently available.

F.1.4 Initial Findings

1. A few of the smaller associations that serve the Energy Sector consider themselves too small to offer security training to their members. They use larger organizations such as the API to provide training.

2. Many training programs require registration fees that may be too costly for smaller companies in the Energy Sector and could limit the number of or prevent their staff members from attending.

3. Training programs are often developed in direct response to legislation or mandates by the Federal Government.

4. Associations focus on preparedness training that seems to correspond closely to their traditional safety and health training programs.

5. Private sector companies that currently provide training services to industry may be the best suited to deliver the desired training to industry.

Table F-1 summarizes findings on Energy Sector training programs. Profiles of each organization's security-related activities follow.

F.2 Oil and Natural Gas Industry Profiles

F.2.1 American Gas Association

F.2.1.1 Security, Integrity, and Reliability Committee

Web site: http://www.aga.org/Committees/gotocommitteepages/sectyintegrityreliabilitycmte/

This committee provides board-level leadership to promote security, infrastructure integrity, and reliability of the Nation's natural gas utility delivery system. It oversees AGA policy in the areas of infrastructure security (physical and cyber) and operational reliability (pipeline safety and integrity management). It has held numerous workshops and forums to discuss and share security information, including the Natural Gas Security Summit, Energy IT Conference and Expo, Operations Conference, Fall Committee Meetings, Special International Security Roundtable, Leadership Conference Calls, Regional Association Conference Calls, SCADA Encryption Workshops, and joint AGA Natural Gas Security Committee and EEI Security Committee meetings.

F.2.1.2 Natural Gas Security Committee

Web site: http://www.aga.org/Committees/gotocommitteepages/naturalgassecurity/

This committee:

- Provides a forum for the identification, development, and communication of innovative and cost effective security solutions for the natural gas industry.

- Provides insight on physical infrastructure security-related pursuits by AGA operating, government relations, and regulatory affairs sections.

- Investigates new technologies as they relate to infrastructure protection.

Table F-1: Summary of Energy Sector Training Programs

Organization	Relevant Committee(s)	Types of Training				Focus
		Workshop/Classroom	Guide/ Manual	Web-based	Forums/ Information Sharing	
Oil and Natural Gas Subsector Associations						
American Gas Association	Security Integrity and Reliability Committee	■				Preparedness
	Natural Gas Security				■	Preparedness
American Public Gas Association	Security and Integrity Foundation	■			■	Preparedness
American Petroleum Institute		■	■			Preparedness
National Petrochemical and Refiners Association	Cyber Security Subcommittee				■	Preparedness
	Security Committee				■	Preparedness
National Propane Gas Association	Propane Emergencies	■	■	■		Response
Independent Liquid Terminals Association		■				Preparedness
Interstate Natural Gas Association of America	Security Committee				■	Preparedness
Electricity Subsector Associations						
American Public Power Association	Safety Committee		■			Preparedness
Edison Electric Institute	Security Committee	■				Preparedness
Electric Power Research Institute	Infrastructure Security Initiative				■	Preparedness
North American Electric Reliability Corporation	Critical Infrastructure Protection Committee	■				Preparedness
Private Organizations						
Response Management Associates, Inc.		■	■	■	■	Preparedness and Response

- Sponsors programs, papers, and presentations at related technical symposiums within the energy industry.

- Develops and publishes committee reports and technical papers. Provides and encourages liaisons with appropriate national and international industry groups, professional associations, and other committees to exchange information and technical assistance with regard to infrastructure protection.

- Establishes a common ground for the promotion and development of viable external relationships with governmental agencies and public law enforcement and emergency response organizations.

F.2.1.3 Cryptographic Protection of SCADA Communication Program

This program defines the data encryption protocol for securing SCADA systems against possible cyber security attacks.

F.2.2 American Public Gas Association (APGA)

F.2.2.1 Security and Integrity Foundation (SIF)

Point of contact: Leonard Phillips, Chairman of APGA Security and Integrity Foundation and Manager of Natural Gas Distribution, City Utilities of Springfield, Missouri, P.O. Box 551, Springfield, MO 65801, Phone: 865-483-1377, email: bpa@orud.org

Web site: www.apgasif.org

SIF is a nonprofit 501(c)(3) corporation. APGA, a 501(c)(6), created SIF in 2004. SIF is dedicated to promoting the security and operational integrity and safety of small natural gas distribution and utilization facilities. SIF focuses on enhancing the ability of gas utility operators to prevent, mitigate, and repair damage to the Nation's small gas distribution infrastructure. It accomplishes this by providing education, training, materials, services, and products specifically designed to increase the knowledge, skills, and abilities of small distribution system and master meter system operators. SIF also focuses on increasing small operators' compliance with DOT operator qualification (OQ) requirements. In initiating, implementing, and expanding its efforts in this regard, SIF works cooperatively with the PHMSA.

F.2.3 American Petroleum Institute (API)

F.2.3.1 Workshop on USCG Regulations for Facility Security Officers (FSOs)

Web site: http://www.api-u.org/FSO.htm

This workshop covers requirements for FSOs that were released in the USCG Final Rule, Part 105, Subpart B. Course materials include a reference CD of more than 30 helpful related documents, including the regulation itself, Navigation and Vessel Inspection Circulars, API's *Security Vulnerability Assessment for the Petroleum and Petrochemical Industries,* and numerous DHS bulletins.

Participants include those interested in understanding or conducting security vulnerability assessments. The program covers all segments of the oil and gas industry: exploration, production, refining, pipeline, and marine. The methodology can be applied to other industries, including the chemical, pharmaceutical, food processing industries.

F.2.3.2 Workshop on Industry Security Vulnerability Assessments (SVAs)

Web site: http://www.api-u.org/SVA.html - DatesLocations

This SVA training focuses on the petroleum, petrochemical, and chemical industries. The objective of an SVA is to identify security hazards, threats, and vulnerabilities facing a facility and to evaluate countermeasures that will provide for the protection of the public, workers, national interests, the environment, and the company. This course provides instruction on how to conduct an SVA to assess security risks and identify potential countermeasures for reducing vulnerabilities. Attendees receive a CD with related documents, including a copy of the API/NPRA publication, *Security Vulnerability Assessment for the Petroleum & Petrochemical Industries.*

F.2.4 National Petrochemical and Refiners Association (NPRA)

F.2.4.1 Cyber Security Subcommittee

This subcommittee advises and assists the Plant Automation and Decision Support Committee and the NPRA board of directors and staff on matters pertaining to cyber security and cyber terrorism that target business and control systems in the refining and petrochemical industries. It solicits and develops recommendations from NPRA members on these matters and ensures that the recommendations are considered by the appropriate governmental bodies and industry groups. It develops cyber security programs that are presented at NPRA cyber security workshops, the Plant Automation and Decision Support Conference, NPRA Annual Meeting, and NPRA Security Conference.

F.2.4.2 Security Committee

This committee advises and assists the Board of Directors and NPRA members with regard to security-related practices and policies, standards and guidelines, and regulatory and legislative trends. It solicits and assembles recommendations from members on these matters and ensures that the recommendations are considered by the appropriate governmental bodies and industry and trade groups. The Security Committee is also responsible for developing the programs for NPRA's security conferences.

F.2.4.3 Annual Security Conference

Web site: http://www.npradc.org/forms/meeting/MeetingFormPublic/view?id=D21500000208

This conference presents current topics of critical importance to help attendees keep up to date on security issues. The exhibition held as part of the conference gives attendees the opportunity to meet and talk with representatives from companies offering a variety of security services to the refining and petrochemical industries.

F.2.4.4 Cyber Security Workshop

This interactive workshop discusses the latest issues in cyber security as it relates to IT and process control systems in the industry. Attendees review and discuss real-life case studies and effective security practices, how to educate the workforce on cyber security, and the latest cyber security tools.

F.2.5 National Propane Gas Association (NPGA)

F.2.5.1 Propane Emergencies Committee/Train-the-Trainer Program

Web site: www.propanesafety.com

NPGA developed a training program on propane emergencies for the fire service. Its primary goal is to improve firefighter safety in responding to propane emergencies. The Propane Emergencies Program curriculum consists of three elements: the Propane Emergencies textbook, a trainer's Facilitator Guide and a dedicated Web site.

Textbook. Funded by industry assessments paid to the Propane Council, NPGA was able to develop a 220-page textbook covering the physical properties of propane, design and construction features of both bulk and non-bulk propane containers, typical emergency scenarios, and tactical guidelines. The textbook has been distributed at no cost to every fire department and propane dealer in the United States.

Facilitator's guide. This guide for trainers supports the Propane Emergencies Program curriculum. The package includes lesson plans for delivery in a 24-, 8-, or 4-hour format. The program is supported by a CD-ROM with lesson plans and interactive training scenarios, as well as overheads, title slides, and a full-scale animated Power Point presentation. The training package is supported by a 50-minute-long video produced by the Emergency Film Group. The first part of the video program explains the various types of propane containers and the second part discusses firefighting tactics.

Web site. The Propane Emergencies Program also has a dedicated Web site, www.propanesafety.com. The site provides an overview of the program, instructional tips, background information on how to make training props, up-to-date changes to lesson plans, and downloadable graphics support for the instructor.

The Propane Council sponsors regional train-the-trainer programs in cooperation with State and local fire training academies. The program is available at no charge. The objective of the one-day program is to introduce qualified fire service instructors to the Propane Emergencies Program's curriculum and support materials.

F.2.6 Independent Liquid Terminals Association

F.2.6.1 Transportation Worker Identification Credential (TWIC) Program

A train-the-trainer program is being developed in response to TWIC regulations.

F.2.7 Interstate Natural Gas Association of America (INGAA)

F.2.7.1 Security Committee

Web site: http://www.ingaa.org/cms/15/3558/4248.aspx

A subcommittee of the Operations, Safety, and Environment (OS&E), the mission of the Security Committee is to:

Monitor and make recommendations on security issues that will affect the interstate natural gas pipeline industry and identify R&D related to those issues.
Identify key rulemakings and initiatives that will have significant impacts on the industry.
Coordinate industry participation in key rulemakings and initiatives to yield more appropriate and workable regulation.

F.3 Electric Power Industry Profiles

F.3.1 American Public Power Association (APPA)

F.3.1.1 Safety Committee

Manual: APPA Safety Manual for an Electric Utility

Point of Contact: Michael Hyland, Phone: 202-467-2986, email: mhyland@APPAnet.org

The committee is responsible for utility safety policies and practices. The committee is also responsible for updating the *Safety Manual for an Electric Utility*.

F.3.2 Edison Electric Institute (EEI)

F.3.2.1 Security Committee

Point of Contact: Laura Hussey, Phone: 202-508-5064

Committee holds workshops in order to exchange security information between its members, NERC, and government agencies. The committee also holds joint meetings with the AGA Security Committee.

F.3.3 Electric Power Research Institute (EPRI)

F.3.3.1 Infrastructure Security Initiative

Point of Contact: Tom Taylor, email: Ttaylor@epri.com

Develops strategies to strengthen and protect electric power infrastructure and outlines plans for rapid recovery from terrorist attacks.

F.3.4 North American Electric Reliability Corporation (NERC)

F.3.4.1 Critical Infrastructure Protection Committee (CIPC)

Point of Contact: Stanley Johnson, Phone: (609) 452-8060, e-mail: stan.johnson@nerc.net

Web site: http://www.nerc.com/~filez/cip.html

CIPC coordinates NERC's security initiatives. The group is comprised of industry experts in the areas of cyber security, physical security, and operational security. CIPC reports to NERC's Board of Trustees. It is governed by an Executive Committee, whose members manage CIPC policy matters and provide support to CIPC's subcommittees and their working groups and task forces.

NERC periodically conducts workshops that explain recent standards approved by Federal Energy Regulatory Commission (FERC), including those related to Cyber Security. NERC's role is to train and educate utility owners and operators on these standards, not how to meet them. Training on meeting the standards is left to owners and operators. NERC auditors will evaluate training programs given by owners and operators to determine if utilities are in compliance with standards.

Note: NERC believes that training should be left to owners and operators, thus Federal involvement is not necessary.

F.4 Private Sector Profiles

F.4.1 Response Management Associates, Inc. (RMA)

RMA provides emergency planning, response, and preparedness services. It specializes in crisis and incident management, planning, training, and consulting and in the design and facilitation of emergency response and crisis simulation exercises and environmental, health, and safety management software.

F.4.1.1 Facility Security Officer (FSO) Workshops

Web site: http://www.rmaworld.com/2007%20FSO%20Flyer.pdf

RMA offers standard-setting security training courses that meet the requirements of 33 CFR Part 105 (USCG) and 49 CFR Part 172 (DOT). These courses provide FSO training that focuses on the FSO, assessment of risks and vulnerabilities, threat identification, and security equipment and systems. They also give facility personnel who have security duties (non-FSOs) basic facility security measures and information.

F.4.1.2 Qualified Individual Training

Web site: http://www.rmaworld.com/2007%20QI%20Flyer.pdf

This training course is designed to prepare the qualified individual (QI) to manage an oil spill incident as the designated QI and/or on-scene incident commander, be fully capable of developing and implementing an action removal plan, and commit the financial resources of the company to prevent or clean up an oil spill. Course topics include the following:

- Roles, responsibilities, and authorities of the QI.
- Applicable governmental regulations.
- Homeland security.
- Media relations.
- Incident/unified command system.
- Crisis management.
- Notification and documentation procedures.
- Facility, area, and national contingency plans.
- Available resources: private and governmental.
- Roles of Federal/State environmental agencies.
- Oil spill response strategies.
- Duties and roles of the spill management team.

F.4.1.3 Spill Prevention Control and Countermeasures (SPCC) Compliance Workshop and Luncheon

Web site: http://www.rmaworld.com/SPCC%20Workshop%20&%20Luncheon%20Flyer-NJ.2.pdf

RMA hosts workshops and luncheons. Industry experts, environmental professionals, and regulators come together to speak about the SPCC Rule.

F.4.1.4 Incident Command System (ICS) Workshops

Web site: http://www.rmaworld.com/2007%20ICS%20Flyer.pdf

These workshops are designed for personnel who are responsible for their facility's spill response program. The objective is to increase their understanding of the program and its application during emergencies. The ICS is an efficient, flexible, and standardized response management system. It provides an "all hazard, all risk" approach to managing the operations that are implemented to respond to crises (e.g., chemical spills, fire, floods, and earthquakes) as well as noncrisis, planned events like concerts.
The ICS was originally developed to address concerns associated with incidents involving multiple agencies, but it applies to any response situation to address both large and small incidents. The ICS allows for resources to be shared effectively, whether a resource comes from the responsible organization, the community, or a local or national agency. An understanding of

the concepts and principles of the ICS allows for logical and smooth organizational expansion and contraction, depending on the scope of the incident. When use of the ICE is planned for and practiced, the ICS will increase the amount of support provided to personnel during incidents.

F.4.1.5 Hurricane and Disaster Response Luncheon

Web site: http://www.rmaworld.com/Hurricane%20and%20Disaster%20Response%20Flyer-Houston.pdf

This RMA luncheon brings together industry experts and environmental, risk, and emergency response professionals to speak about hurricane preparedness, response, and recovery.

F.4.1.6 First Responder Workshop: Operational Level

Web site: http://www.rmaworld.com/Coursedescription.htm — FirstResOL

This class satisfies the 29 CFR 1910.120(q)(6)(ii) requirements for the initial training of hazardous substance emergency responders. Participants who successfully complete this class receive a reference manual, certificate of completion, and laminated wallet card. The workshop covers the following topics:

- Hazard recognition techniques.
- Health hazards and toxicology.
- Medical surveillance programs.
- Emergency response plans.
- Personnel decontamination.
- Dermal and respiratory protective equipment.
- Control, containment, and confinement.

Attendees must pass a written test to demonstrate their understanding of the material

F.4.1.7 First Responder Workshop: Awareness Level

Web site: http://www.rmaworld.com/Coursedescription.htm — FirstResAL

This class satisfies the 29 CFR 1910.120(q)(6)(i) requirements for the initial training of hazardous substance emergency responders. Participants who successfully complete this class receive a reference manual, certificate of completion, and laminated wallet card. The following topics are covered:

- Hazard recognition techniques.
- Health hazards and toxicology.

- Medical surveillance programs.
- Emergency response plans.

Attendees must pass a written test to demonstrate their understanding of the material.

Attachment G: Energy Sector Protective Programs

The following table listing 114 Energy Sector protective programs provides a basic description of the activity and security goal category that each program supports. Further information, when it is available, will be provided to DHS for its Energy Sector critical infrastructure programs database. Program information is currently limited by the Paperwork Reduction Act (*United States Code*, volume 44, pages 3501 et. seq. [44 USC 3501 et seq.]).

Table G-1: Energy Sector Protective Programs

Organization	Name	Description	Type*
*Security goal category supported by program type: A = Information Sharing and Communication, B = Physical and Cyber Security, C = Coordination and Planning, and D = Public Confidence.			
Industry			
AGA (American Gas Association)	Cryptographic Protection of SCADA Communication	Defines a data encryption protocol for securing SCADA systems against possible cyber security attacks.	B
AGA	Natural Gas Security Committee (NGSC)	Provides board-level leadership to promote security, infrastructure integrity, and reliability of the Nation's natural gas utility delivery system. Oversees AGA policy in the areas of infrastructure security (physical and cyber) and operational reliability (pipeline safety and integrity management). Provides a forum for the identification, development, and communication of innovative and cost-effective security solutions for the natural gas industry; provides insight on physical infrastructure security-related pursuits by AGA's operating, government relations, and regulatory affairs sections; investigates new technologies as they relate to infrastructure protection; sponsors programs, papers, and presentations at related technical symposiums within the energy industry; develops and publishes committee reports and technical papers and provides and encourages liaisons with appropriate national and international industry groups, professional associations, and other committees for the exchange of information and technical assistance related to infrastructure protection; and establishes a common ground for the promotion and development of viable external relationships with governmental agencies and public law enforcement and emergency response organizations. It has held numerous workshops and forums to discuss and share security information, including the Natural Gas Security Summit, Energy IT Conference and Expo, Operations Conference, Fall Committee Meetings–Special International Security Roundtable, Leadership Conference Calls, Regional Association Conference Calls, SCADA Encryption Workshops, and joint AGA Natural Gas Security Committee and EEI Security Committee meetings.	A

Table G-1 (Cont.)

Organization	Name	Description	Type*
AGA, INGAA (Interstate Natural Gas Association of America), APGA (American Public Gas Association)	Security Guidelines: Natural Gas Industry, Transmission and Distribution	Provides an approach for vulnerability assessments, critical facility definition, detection and deterrent methods, response and recovery, cyber security, and relevant operational standards.	B, C
API (American Petroleum Institute)	Information Management and Technology Program	Provides a comprehensive review and quantitative assessment of company security programs, focusing on due-care requirements, a database of security programs, and compliance initiatives.	A, B
API	Pipeline SCADA Security Standard (API Standard 1164)	Provides a model for proactive industry actions to improve the security of the Nation's energy infrastructure.	B
API	Security Committee	Has held numerous workshops and forums to share information related to security, including the annual API IT Security Conference for the Oil and Natural Gas Industry, Security Committee meetings (three times a year), API IT Security Forum (ITSF) Committee meetings (quarterly), and the Industry Hurricane Preparedness and Response Conference.	A
API	Security in the Petroleum Industry	Recommends security practices for all segments of the sector.	B
API, NPRA (National Petrochemical and Refiners Association)	Security Vulnerability Assessment for the Petroleum and Petrochemical Industries	Provides practical, hands-on knowledge for performing security vulnerability assessments in multiple industries.	B
APPA (American Public Power Association)	Demonstration of Energy-Efficient Developments (DEED)	DEED is APPA's R&D program. Created in 1980, it is made up of 600-plus APPA member utilities. DEED focuses grants and scholarships in various areas of electric utility operations, including physical and cyber security. The program helped APPA members by producing the APPA Security Checklist and Guidance Manual. This checklist was sent to every electric municipal system operating in the United States, and it gave utilities real-world "effective security practice" examples of how to protect their systems — not of why they should protect their systems.	B
APPA	IT Committee and Listserver	Provides and shares information on IT issues, including security information, at regularly scheduled meetings at the APPA Business and Finance Conference.	A

Table G-1 (Cont.)

Organization	Name	Description	Type*
APPA	Reliable Public Power Provider (RP3) Program	RP3, launched in 2005, recognizes APPA member utilities that meet stringent guidelines and levels of attainment in the areas of reliability, safety, cyber security, mutual aid, disaster management, R&D, and system improvement. As of April 2008, 132 APPA members earned their RP3, representing 26 percent of customers. This self-diagnostic approach forces municipal utilities to show they are addressing areas of DOE/DHS concern. Areas such as disaster management and preparedness (including NIMS), NERC standards and registration, cyber and physical security planning, and mutual aid are all part of the graded application.	D
APPA	Security Committee and Listserver	Provides and shares information within the APPA member communities. Holds meetings at the APPA Engineering and Operations Technical Conference. APPA has leveraged its electronic database of utility information to form a security list serve/committee that has grown over time to convey important messages from DOE, DHS, and NERC and to forge discussions on utility concerns, questions, and effective security practices development. This interest from the membership has also led APPA to run utility education classes aimed at the municipal segment; publish security-based articles in widely read APPA publications such as *Public Power Magazine* and *Public Power Weekly*; and hold security-based presentations at all APPA-run workshops and conferences.	A
EEI (Edison Electric Institute)	Business Continuity Task Force (CEO Level) and Working Group (Staff Level)	Works to develop a shared understanding of business continuity and emergency management. Develops and shares effective security practices within the electric industry. Holds conferences and workshops, including several specific to pandemic planning.	A, C
EEI	IT Working Group, Security Committee	Provides information and develops strategies to help electric utilities address cyber security threats; holds joint meetings and prepares white papers on software patch management and risk vulnerability assessments.	A
EEI	Security Committee	Holds workshops and forums to facilitate security information exchange among its members, NERC, and government agencies, as well as joint AGA Natural Gas Security Committee and EEI Security Committee meetings.	A, C
EEI and a large group of electric utilities	Spare Transformer Sharing Agreement	More than 40 transmission facility owners developed and signed a spare transformer sharing agreement designed to require participants to maintain a specified number of high-voltage spare transformers and provide them to other participants if an act of terrorism occurs. The spare transformers may also be used for other mutual assistance efforts. In all cases, spares that are placed in service must be replaced. On September 21, 2006, FERC issued an order granting certain authorizations that were requested by the signatories to facilitate operation of the agreement and encourage additional participation.	B, C
Electric Power Research Institute (EPRI)	Electricity Infrastructure Security Assessment	Provides a preliminary analysis of potential terrorist threats to the North American electric system, together with some suggested countermeasures.	B
EPRI	Infrastructure Security Initiative	Develops strategies to strengthen and protect the electric power infrastructure and outlines plans for rapid recovery from terrorist attacks.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
INGAA	Security Committee	Runs SCADA security workshops.	A
The Infrastructure Security Partnership (TISP)	Guide for an Action Plan to Develop Regional Disaster Resilience	Developed by a TISP task force of more than 100 practitioners, policymakers, and technical and scientific experts from across the Nation, this guide provides a strategy for communities to develop the level of preparedness needed to manage major disasters. The guide is intended for all organizations with specific missions or a vested interest in ensuring that the regions in which they reside can withstand major disasters and respond and recover rapidly.	C
NERC (North American Electric Reliability Council)	Critical Infrastructure Protection Committee (CIPC)	Composed of industry experts in the areas of cyber, physical, and operational security, CIPC coordinates NERC's security initiatives.	A, B, C
NERC	Cyber Security Standards	Provides reliability standards for the classification of information, identification and protection of critical cyber assets, and reporting of process control and SCADA and incidents. Electric industry cyber security standards are compliance based and required by FERC and the new Electric Reliability Organization (ERO).	C
NERC	Electricity Sector Information Sharing and Analysis Center (ESISAC)	The ESISAC serves the Electricity Subsector by facilitating communication between subsector participants, the Federal Government, and other critical infrastructures. It is the job of the ESISAC to promptly disseminate threat indications, analyses, and warnings, together with interpretations, to help Electricity Subsector participants take protective actions.	A
NERC	Industrywide Critical Spare Equipment Database	Informs companies of the location and technical characteristics of available spare transformers.	B, C
NERC	Influenza Pandemic Planning, Preparation, and Response Reference Guide	For use by Electricity Subsector owners and operators, it develops contingency plans in the event of a flu pandemic. A new threat is the possibility of an influenza pandemic caused by the H5N1 virus. The virus is currently infecting large populations of birds in Asia. It has also infected human beings, with fatal results. It is reported to be spreading rapidly in domesticated birds and birds in nature. It has attracted the serious attention of governments and health organizations throughout the world. Regardless of what happens with the H5N1 strain, all medical experts agree that an influenza pandemic will occur in the future, and the Electricity Subsector's business continuity plans need to address this threat.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
NERC	Risk Assessment Methodologies for Use in the Electric Utility Industry	This study by the NERC Risk Assessment Working Group provides an overview of risk assessment approaches and guidance on risk assessment methods applicable to the Electricity Subsector. It is available at www.esisac.com/ library-assessments.htm. It includes a basic approach for assessing the risk and vulnerability of an electric company's key facilities by EEI's Security Committee, a risk assessment methodology for dams and one for transmission, and security vulnerability self-assessment guidelines for the electric power industry that provide guidance, templates, and checklists to assess security vulnerability. In 2002, NERC's CIPC issued security guidelines on vulnerability and risk assessments for the Electricity Subsector. This document is a supplement to the 2002 guidelines and provides summary information on security risk assessments.	B
NERC	Time-Stamping Guideline	Develops physical security and business network electronic connectivity.	B
NWPP (Northwest Power Pool), WECC (Western Energy Coordination Council)	Reliability and Coordination Programs	NWPP and WECC coordinate to maintain member-utilities' ability to manage risk and implement effective security, system reliability, and recovery efforts as needed to ensure public confidence. NWPP, a subset of WECC, serves as a forum in the electrical industry for reliability and operational adequacy issues in the Northwest for the transition period of restructuring and for the future. NWPP promotes cooperation among its members to achieve reliability in the operation of the electrical power system, coordinate power system planning, and assist in transmission planning in the Northwest Interconnected Area. It is a voluntary organization composed of major generating utilities serving the Northwestern United States, British Columbia, and Alberta. NWPP was originally formed in 1942, when the Federal Government directed utilities to coordinate operations in support of wartime production. NWPP activities are largely determined by major committees: Operating Committee, Pacific Northwest Coordination Agreement (PNCA) Coordinating Group, and Transmission Planning Committee. WECC was formed on April 18, 2002, by the merger of the Western Systems Coordinating Council (WSCC), Southwest Regional Transmission Association (SWRTA), and Western Regional Transmission Association (WRTA). The formation was accomplished over 4 years through the cooperative efforts of WSCC, SWRTA, WRTA, and other regional organizations in the West. WECC's interconnection-wide focus is intended to complement current efforts to form regional transmission organizations (RTOs) in various parts of the West. WECC is responsible for coordinating and promoting electric system reliability, as had been done by WSCC. In addition, WECC will support efficient competitive power markets, assure open and nondiscriminatory transmission access among members, provide a forum for resolving transmission access disputes, and offer an environment suitable for coordinating the operating and planning activities of its members, as set forth in the WECC bylaws.	C, D
NPRA	Cyber Security Subcommittee	Advises and assists the Board of Directors on cyber security and cyber terrorism that targets business and control systems in the refining and petrochemical industries.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
NPRA	Security Committee	Has held several workshops, tabletop exercises, and conferences to share effective security practices, including annual security conferences; workshops and forums on implementing the MTSA; the 2006 Gulf Coast Labor Outlook; TWIC Program; and training courses for FSOs on complying with MTSA.	A, C
Federal Government			
BPA (Bonneville Power Admin-istration)	BPA Initiative	Continues to develop key physical security technologies that can be used for barrier protection and detection sensors for electrical transmission towers and conductors.	B
BPA	Risk Assessment Methodology for Transmission (RAM-T^{SM})	Risk assessment process designed to analyze the current security risks for electrical transmission systems and provide information to support effective risk reduction decisions. RAM-T^{SM} is a way to systematically characterize and assess the security requirements of the Nation's electrical transmission system facilities to deter, prevent, and mitigate malevolent attacks. The methodology and training are available to owners, operators, managers, and others responsible for transmitting electrical power.	B
Canadian Electricity Association, DHS, DOE, NERC, NRCAN (Canadian Department of Natural Resources), PSEPC (Public Safety and Emergency Preparedness Center)	International Electricity Infrastructure Assurance Forum	Using the expertise of others in the areas of policies, practices, technology, R&D, and incident analysis, this forum helps address the vulnerabilities and interdependencies of electricity infrastructures. It is a collaboration of Australian, Canadian, New Zealander, U.K., and U.S. security partners and government agencies.	A, C
DHS-FEMA (Federal Emergency Management Agency)	Federal Hazard Mitigation Program	Consists of three programs that provide funds for activities that reduce losses from future disasters or help prevent catastrophes: Flood Mitigation Assistance Program, Hazard Mitigation Grant Program, and Predisaster Mitigation Program.	B
DHS-Office of Grants and Training	TOPOFF (Top Officials)	A national-level domestic and international exercise series designed to produce a more effective, coordinated, global response to terrorism involving weapons of mass destruction (WMD). The challenging, role-playing exercises involve the senior Federal, State, and local officials who would direct crisis management and consequence management response to an actual WMD attack.	A, C
DHS-NCSD (National Cyber Security Division)	Control Systems Security Initiative	Provides coordination among Federal, State, local, and tribal governments and control system owners, operators, and vendors to improve control system security within and across all CIKR sectors.	B, C

Table G-1 (Cont.)

Organization	Name	Description	Type*
DHS-NCSD	Federal Cyber Security Systems Programs	DHS established GFIRST to facilitate information sharing and cooperation across Federal agencies responsible for cyber system readiness and response. The members work together to understand and manage computer security incidents and encourage proactive and preventive security practices.	A, B
DHS-NCSD	Priority Telecom-munications	Gives the priority in call completion and access to entities with national security and emergency preparedness missions.	A, B, D
DHS-NCSD, DOE-OE (Office of Electricity Delivery and Energy Reliability), PSEPC, NRCAN, private sector	Roadmap to Secure Control Systems in the Energy Sector (Roadmap)	Provides a strategic framework, goals, and milestones for public-private partnerships to secure control systems. The Roadmap's vision is that in 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.	A, B, C
DHS-IP (Office of Infrastructure Protection)	Critical Infrastructure Partnership Advisory Council (CIPAC)	Provides the operational mechanism for carrying out the sector partnership structure between the GCCs and SCCs.	A
DHS-IP	Comprehensive Review Program	DHS's Comprehensive Review Program reviews selected CIKR across the Nation, in partnership with local authorities and owners and operators, by examining existing security practices and capabilities at all levels across multiple sectors. Initial efforts have focused on nuclear and LNG assets. DOE is an active program participant. The program considers potential terrorist actions for an attack, the consequences of such an attack, and the integrated preparedness and response capabilities of the owner and operator and local law enforcement and emergency response organizations.	B, D
DHS-IP	Homeland Security Information Network (HSIN)	Provides a national Web-based platform to share homeland security information with sector security partners. This information sharing is accomplished horizontally across the U.S. Government, vertically among Federal, State, and local governments, and with the private sector and citizens as outlined in the President's National Strategy for Homeland Security. The network enhances secure reporting and information sharing among participants.	A, B, C
DHS-IP	Infrastructure Information Collection Division (IICD)	A repository for information on assets, systems, and networks that make up the Nation's infrastructure.	A
DHS-IP	Methodology Development	DHS's assessment efforts support improved methodologies for possible use by asset owners and operators.	B
DHS-IP	Protected Critical Infrastructure Information (PCII) Program	Seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of these infrastructures and government entities with infrastructure protection responsibilities. The goal is to reduce the Nation's vulnerability to terrorism.	A
DHS-IP	Site Assistance Visits (SAVs)	Visits to critical infrastructure facilities by protective security professionals, subject-matter experts from SSAs, and local law enforcement personnel to help asset owners and operators assess vulnerabilities at their facilities.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
DHS-IP, Office of Grants and Training	Buffer Zone Protection Program (BZPP)	Grant program designed to provide resources to State, local, and tribal law enforcement officials to facilitate the identification of vulnerabilities and discussions on mitigation between security partners and individual owners and operators.	B
DHS-S&T (Science and Technology) Directorate	DRAFT National Plan for Research and Development in Support of Critical Infrastructure Protection	This is a joint plan with the Executive Office of the President, Office of Science and Technology Policy, on using emerging technology to help mitigate risk to critical infrastructures. The plan is structured around detection and sensor systems; protection and prevention; entry and access portals; insider threats; analysis and decision support systems; response, recovery, and reconstitution; new and emerging threats and vulnerabilities; advanced infrastructure architecture and system design; and human and social issues.	A
DHS-S&T, DOD, DOE, Department of State, FBI	Technical Support Working Group (TSWG)	This U.S. national forum identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. It rapidly develops technologies and equipment to meet the high-priority needs of the terrorism-combating community and addresses joint international operational requirements through cooperative R&D with major allies.	B
DHS-TSA (Transportation Security Administration)	Pipeline Corporate Security Review (CSR)	The CSR Program is an on-site security review with a pipeline company. CSRs help establish working relationships with key security representatives in the pipeline industry and provide TSA with a general understanding of a pipeline operator's security planning and implementation. Data obtained from CSRs will help establish a baseline against which to evaluate minimum security standards in the pipeline industry and will help identify coverage gaps.	B
DOE-OE	Emergency Support Function 12 (ESF-12)	Provides for the effective use of available electric power, natural gas, and petroleum products required to meet essential needs, and facilitates restoration of energy systems affected by an emergency or disaster.	C
DOE-OE, ISER (Office of Infrastructure Security and Energy Restoration)	ISERnet	A secure communications network for State and local government personnel who have access to information on energy supply, demand, pricing, and infrastructure. Members include representatives from State energy offices, public utilities, State legislatures, State EM agencies, State homeland security offices, and governors' offices. The ISERnet Web site provides a secure information-sharing network for Energy Emergency Assurance Coordinators (EEAC) System members, allowing them to communicate with each other to identify and address emerging energy supply disruptions and emergencies. During emergencies, this coordination has served as an imperative mechanism for response and cooperation among State decisionmakers.	A, C
DOE-OE	National SCADA Test Bed (NSTB) Program	The joint DOE laboratory program develops and implements the SCADA Vulnerability Assessment Tool and improves cyber security of the electric power grid by assessing energy control systems and identifying potential vulnerabilities to cyber attack.	B
DOE-OE	Visualization and Modeling Working Group (VMWG)	Provides visualization, modeling, and analysis of critical energy infrastructures to prepare for natural disasters and support post-disaster recovery efforts.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
DOE-CIP Board	21 Steps to Improve the Cyber Security of SCADA Networks	The President's CIP Board and DOE developed these steps to help any organization improve the security of its SCADA networks. The steps are not prescriptive or all-inclusive, but they do address essential actions to be taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.	B
DOE-PMAs (Power Marketing Administra-tions)	PMA Emergency Management (EM) Program	Establishes specific EM policy and requirements for DOE PMAs that are appropriate for their specific regional power missions. This program is compatible with DOE's EM system and with the emergency preparedness and disaster reporting requirements of the electric utility industry. Exercises include TOPOFF, Forward Challenge, Pacific Peril, Cascade Lightning, and Blue Cascades.	C
DOE, DHS-TSA, FERC, DOD, DOT, trade associations	Natural Gas Pipeline Regional Disruption Project	Determines the natural gas market's ability to absorb and reallocate gas supplies in the event of a significant pipeline disruption. Specifically, the study aims to determine the market's ability to withstand loss of regional pipeline transportation capacity without causing an outage to residential and commercial customers during peak and other usage periods and forcing a "re-light" in large parts of the system.	B
DOT-PHMSA (Pipeline and Hazardous Materials Safety Admin-istration)	Pipeline Security Information Circular	Defines critical pipeline facilities, identifies appropriate countermeasures for protecting them, and explains how PHMSA plans to verify that operators have taken appropriate action to implement satisfactory security procedures and plans.	A, B
FBI (Federal Bureau of Investigation)	InfraGard	An information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. InfraGard is a partnership between the FBI and private sector, as well as an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.	A, D
FERC (Federal Energy Regulatory Commission)	FERC Initiative	Oversees NERC and establishes and enforces mandatory electricity reliability standards. Among many other activities, develops and implements guidance to the hydropower industry for self-assessment and security evaluation purposes.	B
IFIP (Inter-agency Forum for Infrastructure Protection	IFIP	Created in 1997, IFIP is a consortium of Federal agencies that represent power dam owners, transmission system operators, and anti-terrorism/security experts. IFIP's mission is to (1) promote information exchange between Federal dam owners and operators and the Federal PMAs on security issues in order to identify effective solutions to common problems regarding critical national infrastructure, (2) improve interagency and cross-sector communications and threat reporting, and (3) provide opportunities for government and private sector organizations to cooperate in identifying and resolving national security and CIP issues. DOE's PMAs (e.g., BPA, Western Area Power Administration, and Southwestern Power Administration) and national laboratories (e.g., Argonne, Idaho, Lawrence Livermore, Pacific Northwest, and Sandia National Laboratories), as well as the U.S. Army Corps of Engineers (USACE), FBI, DOI's Bureau of Reclamation, and the Canadian government, have been leaders in this partnership.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
IFIP Partners and USACE, Intelligence and Security Counter-measures Branch	Incident Reporting System Program	Provides a uniform system to assure timely, complete, and accurate reporting and storing of information on operating incidents at DOE and contractor facilities. Shares threat, warning, and point analyses.	B
International	North American Energy Working Group (NAEWG) Ad Hoc CIP Forum	U.S., Canadian, and Mexican government effort to promote a more fully integrated energy market in North America.	C
International (DHS, DOE)	Security and Prosperity Partnership for North America (SPP)	The SPP provides a vehicle by which the United States, Canada, and Mexico can identify and resolve unnecessary obstacles to trade and a means for improving their response to emergencies and increasing their security, thus benefiting and protecting Americans. The SPP is a trilateral initiative to promote the shared commitment of the Federal Governments of Canada, Mexico, and the United States to a secure and robust critical infrastructure, including the Energy, Transportation, and other sector infrastructures. In 2005, the North American Energy Working Group was made part of this program.	C
National Security Telecom-munications Advisory Committee	Telecommuni-cations and Electric Power Interdependency Task Force	Determines the national security and emergency preparedness concerns associated with interdependency of the telecommunications and electric power infrastructures, focusing on the operational issues between them and how these interdependencies will affect the future of the telecommunications network.	A, C
North American Energy Standards Board	Energy Sector Business Practices and Electronic Communications Standards	Standards for the wholesale and retail natural gas and electricity industries are set by some 300 companies and organizations that participate in the natural gas and electricity markets. DOE's Office of Fossil Energy (FE) supports efforts of this board to ensure that potential issues are addressed before the standards are implemented.	A, B, D
USACE	Threats and Suspicious Incidents (TSI) Program	Program developed for USACE personnel to report anomalies or observations that are suspicious when compared to the normal state of activity. TSIs are raw, unvalidated information that may or may not be related to an actual threat and by their very nature may be fragmented or incomplete. TSIs are categorized into seven incident types, following the Threat and Local Observation Notice (TALON) model: Surveillance, Elicitation, Overflights, Weapons Discovery, Bomb Threat, Suspicious Activity, or Test of Security. TSI information is shared with sector partners and organizations throughout the intelligence and homeland security community. TSIs are an excellent tool for providing timely domestic intelligence and satisfying several of the USACE Commander's Critical Information Requirements (CCIRs).	C
USCG	Area Maritime Security Committees (AMSCs)	Formed as a result of the MTSA of 2002, and composed of Federal, State, local, and private authorities, the committees enhance security efforts in about 50 major ports by helping the Captain of the Port coordinate planning, information sharing, and other necessary activities.	B
USCG	Port Security Inspections	Scheduled visits of waterfront facilities regulated by the MTSA.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
USCG Maritime Members	Area Maritime Security (AMS) Plans	All facilities and vessel owners regulated by MTSA have USCG-approved security plans. Federal Maritime Security Coordinators (FMSCs) focus on preparing AMS Plans. The AMSCs are charged with advising the FMSC on maritime security matters, including the initial development and review of AMS Plans.	B
U.S.-Canada Task Force on the Power System Outage	2003 U.S.-Canada Blackout	This study investigated and reported the causes of the blackout and outlined all actions taken to prevent future blackouts, reduce the scope of those that do occur, and improve the security of the North American electric power grid (www2.nrcan.gc.ca/es/erb/erb/english/View.asp?x=690&oid=1221).	A, C
U.S. National Guard Bureau	HLD-E CAM Methodology; DOE-developed Power Plant and Refinery Annexes	The Bureau cooperates with the National Guard's Joint Interagency Training Center in West Virginia to perform physical vulnerability assessments of select energy facilities. In April 2007, there were six CIP-Mission Assurance Assessment pilot teams: California, Colorado, Georgia, Minnesota, New York, and West Virginia.	B
State, Local, and Tribal Governments			
DOE-OE First Responders	Emergency Response Training Program	Trains a range of security partners in responding to energy emergencies.	C
NARUC (National Association of Regulatory Utility Com-missioners)	Cost Recovery for Energy Assurance	Analyzes policies and practices at the State level that can permit utilities to recover the cost of energy assurance measures that they implement. Cost recovery policies support utility investment in critical infrastructure. Training for public utilities on these issues has also been provided.	C
NARUC	Mapping the Impacts of a Disaster on Natural Gas and Electric Supplies and Demand (Natural Gas Curtailment Tool)	Quick-reference online resource that enables a comparison of natural gas curtailment policies. States can examine how individual policies might trigger unintended natural gas and electricity supply consequences across adjacent States or even across the country (www.naruc.org/gascurtailment).	A
NARUC	Natural Gas Curtailment Plans and Authorities	Assess natural gas curtailment plans and authorities at the State level to identify areas of improvement and foster regional coordination.	C
NARUC	Technical Briefs	Identify key strategies for consideration in dealing with challenges involving the electricity, natural gas, water, and telecommunications infrastructures. Provide public utility commissioners and other participants in the regulatory policy community with introductory overviews, suggested protocols, and additional resources on CIP issues (www.naruc.org/cipbriefs).	A, B, C, D
NARUC, NASEO (National Association of State Energy Officials)	State Energy Assurance Planning Guidelines	Help States revise their existing energy emergency plans to incorporate more robust energy security and CIP components. Security experts work with States to review current plans and amend them to address reliability, resiliency, and security of the energy infrastructure, including sector interdependencies (www.naseo.org/committees/energysecurity/documents/energy_assurance_guidelines_v2.pdf).	C

Table G-1 (Cont.)

Organization	Name	Description	Type*
NCSL (National Conference of State Legislators)	Energy Emergency Training and Simulations	Tabletop training seminars for State legislators allow decisionmakers to observe what occurs in an energy emergency, understand the implications of an energy disruption, and track the information and coordination needed to respond. They enable legislators to make educated and effective policy decisions that significantly impact the strength of CIP in their State.	C
NARUC, NASEO, NCSL, NGA, PTI (Public Technologies Institute)	EEAC and EIAC Systems (Energy Emergency Assurance Coordinators and Energy Industry Assurance Coordinators Systems)	The EEAC system establishes a secure, cooperative communications environment for State and local government personnel who have access to information on energy supplies, demand, pricing, and infrastructure. The Energy Industry Assurance Coordinators (EIAC) system provides threat awareness and security analyses for industry personnel.	A, C
NARUC, NASEO, NCSL, NGA, PTI	Regional Energy Exercises	Regional (multi-)energy emergency exercises for representatives of Federal, State, and local governments and industry. Participants react to scenarios, address actions they would take, review jurisdictional issues, and examine interdependencies. Participants return to their States with tools to enhance protection and response capability.	C
NARUC, NCSL	Information Disclosure Briefings	Briefings give public utility commissions a framework to deal with information disclosure; review State regulatory disclosure issues (including their relationship to FERC), prepare briefing papers on disclosure, and create an inventory of State authorities. A new activity/report is underway to help commissions deal with disclosure issues. Briefings also give legislators a greater understanding of disclosure issues and needs.	A
NASEO	Web-based Education	Provides training and exercises for State energy officials responsible for energy emergency preparedness and response.	A
NCSL	State Energy Assurance Measures, Legislator Tools, and Policy Analysis	Series of succinct publications to educate legislators on CIP issues and allow them to develop effective policies in their States. Includes sample legislation on energy security and assurance issues and policy briefs on cost recovery, information disclosure, and emergency response.	C
NGA (National Governors Association) Center for Best Practices	Energy Assurance Briefings and Guidance	Offer governors and their staffs a concise review of the impacts of energy emergency preparedness and response issues and gives them approaches to consider in developing State energy policy to enhance and address CIP and resiliency issues.	A
NGA Center for Best Practices	State Energy Security Communications and Training Programs	Facilitate a dialogue among State energy officials, homeland security officials, and Federal energy officials. With communications tools, they issue briefs for State decisionmakers and training exercises on energy issues. Address sector interdependencies, CIP, and cooperation among security partners, including jurisdictional issues and effective policy development.	A & C
Pacific Northwest Economic Region (PNWER)	Exercise and Planning	With assistance from the BPA, PNWER is a creation of Pacific Northwest State legislative and provincial governments formed to address CIP and interdependencies across all sectors that impact economic security, national security, and public safety and health. PNWER has conducted a series of regionwide exercises called Blue Cascades. Action plans have been developed to improve protection and preparedness across the PNWER.	C

Table G-1 (Cont.)

Organization	Name	Description	Type*
PTI	Energy Assurance Guidelines for Local Officials	Outlines local government roles in planning for and responding to energy emergencies.	A
PTI and Local Energy Staff and Decision-makers	Energy Emergency Response and Coordination	These individuals coordinate and work with local governments to identify, assess, and respond to evolving energy supply shortages or emergencies, such as the August 2003 blackout and the 2005 hurricane season.	C
State Committees on Homeland Security	Initiatives	These have taken various shapes, depending on the time and effort put into CIP. CIP subcommittees have been established within the committees. They are operated and managed by State EM divisions. Their focus has been on identifying, prioritizing, and protecting critical infrastructure facilities across all sectors.	B, C
Western Area Power Administration	Initiative	This initiative shares information on power and cyber systems and fighting terrorism with the FBI, DHS, and DOI.	A, C
Activities Not in the 2007 Sector Annual Report			
AGA	Natural Gas Mutual Aid Resource Center (NG MARC)	Aids gas utilities in the timely, effective attainment of the person-power and materials needed for efficient service restoration. A culmination of efforts of the utility community, the site gives the user broad access to U.S. utility companies through searchable lists of emergency contact information, field capabilities, and other resources available for mutual assistance.	A, C, D
AGA	Natural Gas Security Guidelines	These are presently being revised by the industry to address the significant progress made by industry and government and highlight the myriad of initiatives underway. The revised guidelines will (a) provide an overview of industry practices that are based on existing and enhanced operational regulations, practices, and processes within the industry; (b) offer an example of a systematic approach for use by companies to determine security risks, implement detection and deterrent practices, and refine response and recovery practices; (c) apply the concept of risk management and, in particular, consequence reduction to address and manage security issues; (d) recognize that many other risk management and vulnerability assessment models are available and that each company must assess risk by using the approach that it finds to be the most effective; (e) provide practices that are general in nature and reflect the importance of flexibility in application by the company; and (f) encourage the natural gas industry to continue to work in a concerted effort with other industries and governmental agencies to effectively manage the security of the industry infrastructure.	A, B, C
API	Annual IT Conference for the Oil and Natural Gas Industry	This second annual IT conference was held on November 6 and 7, 2007, in Houston, Texas. The focus was on security-related topics, including control system security awareness, privacy, identity management, and security/risk implications of data convergence due to virtualization. Conference proceedings are available on a Web site for participants.	A, B, C

Table G-1 (Cont.)

Organization	Name	Description	Type*
API	Information Technology Security Forum (ITSF)	This forum has been in existence for the past 7 years. It focuses on IT security issues that affect the industry. It sponsors an annual IT conference for the oil and natural gas industry (see above). It sponsored the second IT security benchmark survey, which was completed by the fourth quarter of 2007. API has published the first edition of the *API Standard for Third-party Network Connectivity,* which provides guidance for implementing secure third-party connections between the IT systems and networks of two companies that have a business relationship and common objective.	A, B, C
DOE	Joint CIPAC Metrics Working Group	This subgroup was established by the Joint Energy Working Group to address the important subject of metrics. While there is a single subgroup consisting of Energy GCC as well as Oil and Natural Gas and Electricity SCC members, the approach to metrics development differs by subgroup.	A, C, D
DHS-IP	C/ACAMS (Constellation/ Automated Critical Asset Management System)	Secure, Web-based portal designed to help State and local first responders, emergency managers, and homeland security officials collect and organize CIKR asset data as part of a comprehensive CIKR protection program. Provides comprehensive infrastructure inventory management and vulnerability assessment tools, role-based access, standard and customized reports, asset manager questionnaires, BZPP development tools, CIKR asset taxonomy classification capability, electronic CIKR reference library, mapping and geospatial functionality by using the Integrated Common Analytical Viewer (iCAV), and live law enforcement and counter-terrorism news feeds and public disclosure protections through the DHS PCII Program.	B, C, D
DHS-IP	PCIS (Partnership for Critical Infrastructure Security)	Coordinates cross-sector industry/government initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. Its effort spans the full spectrum of critical infrastructure matters, from prevention, planning, and preparedness to business continuity, mitigation, response, and recovery. PCIS focuses primarily on cross-sector policy, strategy, and interdependency issues affecting the critical infrastructure sectors.	A, B, C
DHS	SLTT GCC (State, Local, Tribal, and Territorial Government Coordinating Council)	Consists of State, local, tribal, and Territorial government security partners, who are critical in implementing the NIPP. The SLTT GCC consists of security partners from all CIKR sectors.	A, B, C, D
DHS-IP	CFATS (Chemical Facility Anti-Terrorism Standards)	Program targeting sites housing specified minimum levels of designated chemicals. Will likely impact a significant number of Energy Sector facilities in both the Oil and Natural Gas and Electricity Subsectors.	B
DHS-IP	ECIP (Enhanced Critical Infrastructure Protection)	A new element in the PSAs' efforts. Its purpose is to begin a dialogue between DHS and the asset on the security of the asset. The PSA fills out a questionnaire, with inputs from the asset, which may be submitted voluntarily by the site as part of the PCII Program.	B

Table G-1 (Cont.)

Organization	Name	Description	Type*
DHS-IP	iCAV (Integrated Common Analytical Viewer)	A secure, Web-based geospatial analytical and situational awareness system, consisting of government-owned and licensed data, imagery, and dynamic, mission-specific information integrating threats, weather, and situational awareness information. Provides a geospatial context for a wide variety of information systems, fusing information and providing situational awareness by tracking real-time events. This fusion provides Federal, State, and local jurisdictions and the private sector with a rapid, common understanding of the relationships between events to support coordinated preparedness, response, and recovery activities.	A
DHS-S&T (Science and Technology) Directorate	Recovery Transformer Program	Pilot being initiated in cooperation with DOE to develop a recovery transformer for the electric power industry. This was identified by industry as a critical R&D need.	B, C
DOE	ieRoadmap (Interactive Energy Roadmap)	Web-based tool that allows principal investigators to register and self-populate a database that links to the challenges identified in the Roadmap. The ieRoadmap (hosted on the Process Control Systems Forum Web site www.pcsforum.org) provides a mechanism to encourage collaboration, identify active areas of work, expose gaps, enable partners to leverage resources, and inform owners and operators of emerging technologies.	C
DOE-OE	ISER International Program	OE is the principal DOE element for implementing a number of international activities in cooperation with foreign energy security partners. An international team has been created within ISER.	A, B, C
DOE-OE	Real-time Grid Visualization	Cooperative government/industry real-time effort to monitor and visualize high-voltage transmission lines.	A, C, D
DOE-FE	Coal R&D Programs	Ensure that indigenous coal resources can continue to enable economic development and be transformed to liquids to guard against import dependence and price shocks.	B
DOT	Committee on the Marine Transportation System (CMTS)	Established by the President's Ocean Action Plan in December 2004 to create a partnership of Federal agencies with responsibility for the Marine Transportation System (MTS): waterways, ports, and their intermodal connections. CMTS objectives are to ensure the development and implementation of national MTS policies consistent with national needs and to report its views and recommendations for improving the MTS to the President.	A, C
ILTA (International Liquid Terminals Association)	Security Working Group	Addresses a broad regulatory agenda, including energy, through its Environmental, Health, Safety, and Security Committee. The group has also been addressing a number of issues of concern to its members as they relate to CFATS and the TWIC Program, applicable to MTSA-covered facilities.	A, B, C
NPRA	*Security Watch*	A weekly digest of important security-related events, announcements, and background stories from government and industry.	A, C
NPRA	White Paper on Hurricane Security Operations	Publication providing recommendations for security planning in the event of a hurricane.	A, B, C
NRECA (National Rural Electric Cooperative Association)	Reliability Task Force (RTF)	New task force of member cooperatives focused on reliability issues, including CIP issues. Includes representatives from distribution and generating and transmission cooperatives.	A, B, C

Table G-1 (Cont.)

Organization	Name	Description	Type*
DOE-OE	Electricity Advisory Committee	Created in 2008, the 30-member group advises DOE on a wide range of strategically important electricity issues.	A, B, C, D
DOE-FE, Office of Petroleum Reserves	SPR (Strategic Petroleum Reserve) Program	Owns and operates four storage sites, two in Texas and two in Louisiana, with a combined storage capacity of 727 million barrels. The sites are maintained in a high operational readiness posture, capable of responding to an oil supply disruption at a maximum release rate of 4.4 million barrels per day within 15 days after a Presidential Decision.	B, D
TVA (Tennessee Valley Authority)	TVA	Provides for river navigation, flood control, and agricultural and industrial development and promotes the use of electric power in the Tennessee Valley region.	B, C
USDA (U.S. Department of Agriculture)	Rural Development Electric Programs	Provide reliable and affordable electricity for rural residents. The programs provide capital to upgrade, expand, maintain, and replace America's vast rural electric infrastructure. Under the authority of the Rural Electrification Act of 1936, the programs make direct loans and loan guarantees to electric utilities to serve customers in rural areas.	B, C

Attachment H: NERC Reliability Standards — Status and Sector Goal Category[16]

Standard Number	Title	Security Goal Category*	Approval Date
*Security Goal Categories: A = Information Sharing and Communication, B = Physical and Cyber Security, C = Coordination and Planning, and D = Public Confidence			
Resource and Demand Balancing			
BAL-001-0	Real Power Balancing Control Performance	C	06/07
BAL-002-0	Disturbance Control Performance	C	06/07
BAL-STD-002-0	Operating Reserves (WECC)	C	06/07
BAL-003-0	Frequency Response and Bias	C	06/07
BAL-004-0	Time Error Correction	C	06/07
BAL-005-0	Automatic Generation Control	C	06/07
BAL-006-1	Inadvertent Interchange	C	06/07
Communications			
COM-001-1	Telecommunications	A	06/07
COM-002-2	Communications and Coordination	A	06/07
Critical Infrastructure Protection			
CIP-001-1	Sabotage Reporting	A, B	06/07
CIP-002-1	Cyber Security — Critical Cyber Asset Identification	A, B	01/08
CIP-003-1	Cyber Security — Security Management Controls	A, B	01/08
CIP-004-1	Cyber Security — Personnel and Training	A, B	01/08
CIP-005-1	Cyber Security — Electronic Security Perimeter(s)	A, B	01/08
CIP-006-1	Cyber Security — Physical Security of Critical Cyber Assets	A, B	01/08
CIP-007-1	Cyber Security — Systems Security Management	A, B	01/08
CIP-008-1	Cyber Security — Incident Reporting and Response Planning	A, B	01/08
CIP-009-1	Cyber Security — Recovery Plans for Critical Cyber Assets	A, B	01/08
Emergency Preparedness and Operations			
EOP-001-0	Emergency Operations Planning	C	06/07
EOP-002-2	Capacity and Energy Emergencies	C	06/07
EOP-003-1	Load Shedding Plans	C	06/07
EOP-004-1	Disturbance Reporting	A, C	06/07
EOP-005-1	System Restoration Plans	C	06/07
EOP-006-1	Reliability Coordination — System Restoration	C	06/07
EOP-008-0	Plans for Loss of Control Center Functionality	C	06/07
EOP-009-0	Documentation of Blackstart Generating Unit Test Results	C	06/07
Facilities Design, Connections, and Maintenance			
FAC-001-0	Facility Connection Requirements	C	06/07
FAC-002-0	Coordination of Plans for New Generation, Transmission, and End User	C	06/07
FAC-003-1	Vegetation Management Program	B	06/07

16 Source: NERC, June 20, 2008. Security Goal Categories provided by DOE.

Standard Number	Title	Security Goal Category*	Approval Date
FAC-008-1	Facility Ratings Methodology	C	06/07
FAC-009-1	Establish and Communicate Facility Ratings	A, C	06/07
FAC-010-1	System Operating Limits Methodology for the Planning Horizon	A, C	02/08
FAC-011-1	System Operating Limits Methodology for the Operations Horizon	A, C	02/08
FAC-013-1	Establish and Communicate Transfer Capabilities	A, C	06/07
FAC-014-1	Establish and Communicate System Operating Limits	A, C	02/08
Interchange Scheduling and Coordination			
INT-001-2	Interchange Information	A	06/07
INT-003-2	Interchange Transaction Implementation	C	06/07
INT-004-1	Dynamic Interchange Transaction Modifications	C	06/07
INT-005-1	Interchange Authority Distributes Arranged Interchange	C	06/07
INT-007-1	Interchange Confirmation	C	N/A
INT-009-1	Implementation of Interchange	C	06/07
INT-010-1	Interchange Coordination Exemptions	C	06/07
Interconnection Reliability Operations and Coordination			
IRO-001-1	Reliability Coordination — Responsibilities and Authorities	C	06/07
IRO-002-1	Reliability Coordination — Facilities	A, C	06/07
IRO-003-2	Reliability Coordination — Wide-area View	A, C	06/07
IRO-004-1	Reliability Coordination — Operations Planning	C	06/07
IRO-005-1	Reliability Coordination — Current-day Operations	A, C	06/07
IRO-006-3	Reliability Coordination — Transmission Loading Relief	C	06/07
IRO-STD-006-0	Qualified Path Unscheduled Flow Relief (WECC)	C	06/07
IRO-014-1	Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators	C	06/07
IRO-015-1	Notifications and Information Exchange between Reliability Coordinators	A, C	06/07
IRO-016-1	Coordination of Real-time Activities Between Reliability Coordinators	C	06/07
Modeling, Data, and Analysis			
MOD-006-0	Procedures for Use of CBM Values	C	06/07
MOD-007-0	Documentation of the Use of CBM	A	06/07
MOD-010-0	Steady-state Data for Modeling and Simulation of the Interconnected Transmission System	A, C	06/07
MOD-012-0	Dynamics Data for Modeling and Simulation of the Interconnected Transmission System	A, C	06/07
MOD-016-1	Documentation of Data Reporting Requirements for Actual and Forecast Demands, Net Energy for Load, and Controllable Demand-Side Management	A, C	06/07
MOD-017-0	Aggregated Actual and Forecast Demands and Net Energy for Load	C	06/07
MOD-018-0	Treatment of Nonmember Demand Data and How Uncertainties Are Addressed in the Forecasts of Demand and Net Energy for Load	A, C	06/07
MOD-019-0	Reporting of Interruptible Demands and DCLM Data	C	06/07

Standard Number	Title	Security Goal Category*	Approval Date
MOD-020-0	Providing Interruptible Demands and DCLM Data to System Operators and Reliability Coordinators	A, C	06/07
MOD-021-0	Documentation of the Accounting Methodology for the Effects of Controllable DSM in Demand and Energy Forecasts	C	06/07
Personnel Performance, Training, and Qualifications			
PER-001-0	Operating Personnel Responsibility and Authority	C	06/07
PER-002-0	Operating Personnel Training	C	06/07
PER-003-0	Operating Personnel Credentials	C	06/07
PER-004-1	Reliability Coordination — Staffing	C	06/07
Protection and Control			
PRC-001-1	System Protection Coordination	B	06/07
PRC-STD-001-1	Certification of Protective Relay Applications and Settings (WECC)	B	06/07
PRC-STD-003-1	Protective Relay and Remedial Action Scheme Misoperation (WECC)	B	06/07
PRC-004-1	Analysis and Mitigation of Transmission and Generation Protection System Misoperations	B	06/07
PRC-005-1	Transmission and Generation Protection System Maintenance and Testing	B	06/07
PRC-STD-005-1	Transmission Maintenance (WECC)	B	06/07
PRC-007-0	Assuring Consistency with Regional UFLS Program Requirements	B	06/07
PRC-008-0	Underfrequency Load Shedding Equipment Maintenance Programs	B	06/07
PRC-009-0	Analysis and Documentation of Underfrequency Load Shedding	B	06/07
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load	B	06/07
PRC-011-0	Undervoltage Load Shedding System Maintenance and Testing	B	06/07
PRC-015-0	Special Protection System Data and Documentation	B	06/07
PRC-016-0	Special Protection System Misoperations	B	06/07
PRC-017-0	Special Protection System Maintenance and Testing	B	06/07
PRC-018-1	Disturbance Monitoring Equipment Installation and Data Reporting	A, B	06/07
PRC-021-1	Under-Voltage Load Shedding Program Data	A, B	06/07
PRC-022-1	Under-Voltage Load Shedding Program Performance	B	06/07
Transmission Operations			
TOP-001-1	Reliability Responsibilities and Authorities	C	06/07
TOP-002-2	Normal Operations Planning	C	06/07
TOP-003-0	Planned Outage Coordination	C	06/07
TOP-004-1	Transmission Operations	C	10/07
TOP-005-1	Operational Reliability Information	A, C	06/07
TOP-006-1	Monitoring System Conditions	A, C	06/07
TOP-007-0	Reporting SOL and IROL Violations	A, C	
TOP-STD-007-0	Operating Transfer Capability (WECC)		06/07
TOP-008-1	Response to Transmission Limit Violations	C	06/07

Standard Number	Title	Security Goal Category*	Approval Date
Transmission Planning			
TPL-001-0	System Performance Under Normal Conditions	C	06/07
TPL-002-0	System Performance Following Loss of a Single BES Element	C	06/07
TPL-003-0	System Performance Following Loss of Two or More BES Elements	C	06/07
TPL-004-0	System Performance Following Extreme BES Events	C	06/07
Voltage and Reactive			
VAR-001-1	Voltage and Reactive Control	A, C	06/07
VAR-002-1	Generator Operation for Maintaining Network Voltage Schedules	C	06/07
VAR-STD-002a-1	Automatic Voltage Regulators (WECC)	C	06/07
VAR-STD-002b-1	Power System Stabilizer (WECC)	C	06/07

Attachment I: Pipeline Protective Programs and Initiatives (2008 Update of the Pipeline Modal Annex of the Transportation Systems SSP)

Programs and Initiatives	Description
Pipeline Corporate Security Review Program	The centerpiece of the TSA's pipeline security program is the Pipeline Corporate Security Review (PCSR). Begun in 2003, PCSRs have enabled TSA to build relationships with pipeline operators, assess their corporate security plans and programs, and provide them with recommendations for improvement. TSA has conducted PCSRs on 91 of the top 100 pipeline systems. By the end of this calendar year, TSA will have completed PCSRs on 100 percent of the nation's top 100 pipeline systems.
Cross-Border Pipeline Security Assessments	The pipeline cross-border vulnerability assessments are in support of the Smart Border Accord and the Security and Prosperity Partnership Agreement. Assessment teams of Canadian and U.S. subject matter experts in pipeline operations, control systems, infrastructure interdependencies, and assault planning visit critical cross-border pipeline infrastructures, identify security gaps, and recommend protective measures to mitigate those gaps. Six systems have been reviewed by a joint U.S./Canadian team.
Pipeline Security Forum	TSA, in conjunction with NRCAN, hosted the 2007 International Pipeline Security Forum in Ottawa, Ontario. This international forum provided an opportunity for the U.S. and Canadian Governments and industry pipeline officials to discuss security issues and topics. Attendees included representatives and officials from the U.S. and Canadian Governments, U.S. and Canadian pipeline-related associations, U.S and Canadian pipeline owners and operators, energy and pipeline contractors, and representatives from the security, intelligence, and law enforcement communities. The 2008 International Pipeline Security Forum will be held in Salt Lake City, October 29 and 30, 2008.
Security Awareness Training	The objective of the security awareness training project is to help the pipeline industry achieve the desired levels of employee security awareness through an increased understanding of potential vulnerabilities and threats and of effective security measures to address them. TSA and the pipeline industry have partnered to develop a 30-minute training CD that uses DHS-developed subject matter but is tailored specifically to an audience of pipeline operators. The training covers topics such as security measures, awareness of vulnerabilities, potential threats, and targeting. To date, TSA has delivered training CDs to more than 300 companies, providing training to an estimated 61,000 pipeline employees.
Cyber Attack Awareness and SCADA Security Programs	SCADA systems are designed to relay pipeline performance data to a central control facility and, in some systems, issue commands to remote sites. The Pipeline Security Division is currently working with Johns Hopkins Applied Physics Laboratory to develop a program to identify external weaknesses in company SCADA network security.
Development of the Pipeline Security Guidelines	In September 2002, DOT-Research and Special Programs Administration, Office of Pipeline Safety, issued a pipeline security circular and guidance to improve the security posture of the pipeline industry. TSA is now updating the guidelines in coordination with other government and industry partners.

This page intentionally blank

Attachment J: References and Resources

Agencies and Organizations

DOE-OE (U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability)
Responsible for Energy Sector CIP and energy emergency preparedness
http://oe.energy.gov/.

ISER (Office of Infrastructure Security and Energy Restoration in DOE-OE)
Responsible for ensuring the security, resiliency, and survivability of key energy assets and critical energy infrastructure at home and abroad
http://www.oe.energy.gov/our_organization/iser.htm

NASEO (National Association of State Energy Officials), Energy Data and Security Committee
http://www.naseo.org/committees/energysecurity/index.html.

NARUC (National Association of Regulatory Utility Commissioners), Committee on Critical Infrastructure
http://www.naruc.org/committees.cfm?c=46

NASEO and NARUC, *Energy Assurance Guidelines, Version 2,* Nov. 2005
http://www.naseo.org/committees/energysecurity/documents/Energy_Assurance_Guidelines_v2.pdf

NGA (National Governors Association), Center for Best Practices
http://www.nga.org/portal/site/nga/menuitem.8274ad9c70a7bd616adcbeeb501010a0/?vgnextoid=e9a4d9b834420010VgnVCM1000001a01010aRCRD

NCSL (National Conference of State Legislators), Task Force on Homeland Security and Emergency Preparedness
http://www.ncsl.org/terrorism/Protecting_Democracy.htm

DHS (U.S. Department of Homeland Security)
http://www.dhs.gov/dhspublic/

Documents and Reports

NRF, 2008, DHS-FEMA (Federal Emergency Management Agency), Jan.
Successor to the National Response Plan, it focuses on response and short-term recovery
http://www.fema.gov/emergency/nrf/mainindex.htm#

Emergency Support Function #12 — Energy Annex
http://www.fema.gov/pdf/emergency/nrf/nrf-esf-12.pdf

Critical Infrastructure and Key Resources Support Annex
http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf

The National Infrastructure Protection Plan, 2006, DHS, June
Provides a coordinated approach to CIKR protection roles and responsibilities for government agencies and private sector security partners
http://www.dhs.gov/nipp

Energy Sector-Specific Plan (Energy SSP) Redacted, 2007, DHS and DOE, May
Provides the means to implement the NIPP for Energy Sector CIKR
http://www.oe.energy.gov/DocumentsandMedia/Energy_SSP_Public.pdf

The Governors Guide to Energy Assurance, 2006, National Governors Association (NGA), Center for Best Practices, Dec.
Provides roles and responsibilities for ensuring a robust, secure, and reliable energy infrastructure
http://www.nga.org/portal/site/nga/menuitem.6c9a8a9ebc6ae07eee28aca9501010a0/?vgnextoid=35fe91e19877f010VgnVCM1000001a01010aRCRD

The Role of State Public Utility Commissions in Protecting the National Utility Infrastructure, 2005, National Regulatory Research Institute, Mar.
http://nrri.org/pubs/multiutility/05-03.pdf

National Association of Regulatory Utility Commissioners Technical Briefs on Critical Energy Infrastructure
http://www.naruc.org/cipbriefs

States' Homeland Security Priorities, 2002, NGA, Center for Best Practices, Aug.
http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=d9fc5aa265b32010VgnVCM1000001a01010aRCRD

Roadmap to Secure Control Systems in the Energy Sector, 2006, funded by DOE-OE in collaboration with DHS Science and Technology (S&T) Directorate and Natural Resources Canada, Feb.
http://www.controlsystemsroadmap.net/

Electrical Energy Security, 2002, The Regulatory Assistance Project, Apr.
Part I: Assessing Security Risk
http://www.raponline.org/Pubs/IssueLtr/ElecSec1.pdf
Part II: Policies for a Resilient Network
http://www.raponline.org/Pubs/IssueLtr/ElecSec2.pdf

Emergency Planning and Preparedness: Securing Oil and Natural Gas Infrastructures in the New Economy, 2001, National Petroleum Council, June
http://www.securitymanagement.com/library/NPC_Tech0901.pdf

Pandemic Influenza Resources and Reports

HHS (U.S. Department of Health and Human Services) Pandemic Web site
http://www.pandemicflu.gov

WHO (World Health Organization) Influenza Web site
http://www.who.int/topics/influenza/en/

Preparing for a Pandemic Influenza, 2006, NGA, July
Provides a primer for governors and senior State officials
http://www.nga.org/Files/pdf/0607PANDEMICPRIMER.PDF

National Strategy for Pandemic Influenza, 2005, Office of Homeland Security, Nov.
Provides guidance on U.S. preparedness and response activities to mitigate the impact of a pandemic
http://www.whitehouse.gov/homeland/pandemic-influenza.html

Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources, 2003, DHS, Sept.
Practical tool developed for business owners and operators and their contingency planners to enhance pandemic planning
http://www.pandemicflu.gov/plan/pdf/CIKRpandemicInfluenzaGuide.pdf

This page intentionally blank