Transportation Security Administration

Pipeline Security and Incident Recovery Protocol Plan

March 2010

As directed by the

Implementing Recommendations of the 9/11 Commission Act of 2007

This page intentionally left blank.

FOREWORD

The Pipeline Security and Incident Recovery Protocol Plan (the Plan) is specifically required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act), Pub. L. 110-53. The Plan is drafted in accordance with section 1558 of the 9/11 Act, and with the Annex to the Memorandum of Understanding executed on August 9, 2006, between the Transportation Security Administration (TSA) a component of the Department of Homeland Security (DSH) and the Pipeline and Hazardous Materials Safety Administration (PHMSA) an entity within the Department of Transportation (DOT). The Memorandum of Understanding documents the agreement between DHS/TSA and DOT/PHMSA to seek consensus and cooperation concerning measures to reduce risk and minimize the consequences of emergencies involving pipeline infrastructure. The Plan is also drafted in accordance with the National Strategy for Transportation Security, the National Strategy for Homeland Security, and Homeland Security Presidential Directive-7 concerning critical infrastructure protection.

Section 1558 of the 9/11 Act outlines specific objectives and requirements of the Plan, including:

> "(1) for the Government to provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations as determined under section 1557 when—
>
> (A) under severe security threat levels of alert; or
>
> (B) under specific security threat information relating to such pipeline infrastructure or operations exists; and
>
> (2) an incident recovery protocol plan, developed in conjunction with interstate and intrastate transmission and distribution pipeline operators and terminals and facilities operators connected to pipelines, to develop protocols to ensure the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses in the event of an incident affecting the interstate and intrastate natural gas and hazardous liquid transmission and distribution pipeline system, which shall include protocols for restoring essential services supporting pipelines and granting access to pipeline operators for pipeline infrastructure repair, replacement, or bypass following an incident."[1]

The Plan presents a framework and protocols to support the recovery of pipeline infrastructure, as well as measures to prevent a security incident and enhance resiliency. The purpose of the Plan is to reduce the consequences of an attack, as well as to minimize the operational impact of and time needed to recover from a disruption in the pipeline system infrastructure. It is a phased

[1] P.L. 110-53, § 1558 (a) (2007).

plan that focuses on prevention/protection, response, and recovery measures to be undertaken by the Federal Government supporting State, local and tribal governments and the private sector.

The Plan is the result of a collaborative interagency effort with input from interstate and intrastate transmission and distribution pipeline operators, nonprofit organizations representing pipeline employees, emergency responders, State pipeline safety agencies, public safety officials, and other relevant parties. The continued development of this Plan will be based on the need to reevaluate and enhance current recovery strategies and protocols. The Plan will be updated periodically to address changes in pipeline security threats, technology, and Federal laws and policies.

Table of Contents

Foreword ..... **i**

1 Introduction and Plan Format **1**

1.1 Description of Pipeline Threats 3
1.2 Implications of Disruption of Pipeline Infrastructure 3
1.3 Planning Assumptions 4

2 Roles and Responsibilities **5**

2.1 Federal Role 5
2.2 Federal Role – Key Agencies 5
2.3 Federal Agencies – Supporting Agencies 8
2.4 Tribal, State, and Local Governments and the Private Sector 11

3 Prevention/Protection: Pipeline Security Guidance and Safety Regulations **13**

3.1 Pipeline Security Guidance 13
3.1.2 Industry Guidance 14
3.2 Pipeline Safety Regulations 15
3.2.1 Mandatory Integrity Management Program 15
3.2.2 Special Permits, Safety Orders, and Corrective Action Orders 16
3.3 Additional Planning Considerations 17
3.4 Security of Supervisory Control and Data Acquisition (SCADA) Systems 17

4 Prevention/Protection: Threat Detection and Analysis **19**

4.1 Operations Centers and Information Sharing 19
4.1.1 Overview of Relevant Operations Centers 19
4.1.2 DHS/TSA Interagency Threat Coordination Committee (ITCC) 20
4.1.3 FBI Threat Assessment Process 21
4.1.4 Intelligence Sharing 23
4.1.5 Incident Reporting Originating With Owner/Operators 24
4.2 Pipeline Incident Operations Coordination 24
4.3 Use of Homeland Security Advisory Threat Assessment System for the Pipeline Sector 25
4.3.1 Prevention/Protection Agency Action Chart 28

5 Response **31**

5.1 Overview of Response Considerations 31
5.1.1 On-Scene Pipeline Operations Branch 33
5.1.2 Site Access 34
5.1.3 Response Action Chart 35

6 Recovery **39**

6.1 Recovery Protocols 39
6.1.1 Site-Level Recovery Support 39
6.1.2 National-Level Recovery Support 39
6.1.3 Waivers 41

6.1.4 Responsibilities and Capabilities under the National Response Framework..... 42
6.2 Recovery Agency Action Chart 44
Appendix A: Abbreviations and Acronyms 48
Appendix B: Definitions 52
Appendix C: Authorities 54

List of Figures

Figure 1 Lead Federal Agency Pipeline Incident Continuum 2
Figure 2 FBI Threat Assessment Process 23
Figure 3 Incident Reporting Originating With Owner/Operator 24

List of Tables

Table 1 HSAS Threat Levels and Corresponding DHS/TSA and DOT/PHMSA Actions..... 26
Table 2 Prevention/Protection Action Chart..... 28
Table 3 Response Action Chart 35
Table 4 Recovery Action Chart 44

This page intentionally left blank.

1 INTRODUCTION AND PLAN FORMAT

The Pipeline Security and Incident Recovery Protocol Plan (the Plan) addresses measures to prevent, protect, respond, and recover from a pipeline infrastructure security incident. Pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the 9/11 Act), Pub. L. 110-53, the Plan primarily applies to the Transportation Security Administration (TSA) a component of the Department of Homeland Security (DHS/TSA), and the Pipeline and Hazardous Materials Safety Administration (PHMSA) an entity within the Department of Transportation (DOT/PHMSA). However, the Plan identifies resources other Federal Government agencies can provide to augment security and enhance a pipeline incident recovery. The Plan does not alter existing authorities, but establishes mechanisms for coordination, including processes and protocols, to create a basis for cross-sector actions to recover from a pipeline security incident.

The Plan is organized into three main components corresponding to the primary phases within the homeland security continuum: Prevention/Protection, Response, and Recovery.

For purposes of the Plan, the terms "occurrence" and "event" are synonymous with "incident." Threats or increased threat levels are "incidents" because they require a response to protect life or property. For a complete definition of "incident," as well as definitions for each mission area, see Appendix B.

A security incident is any event determined by DHS/TSA to be significant enough to begin monitoring the situation for further developments. In this sense, the determination that a security event has occurred is discretionary and allows DHS/TSA to be flexible and adapt their actions to a specific set of facts. When a pipeline security incident occurs, a coordinating phone call between DHS/TSA and DOT/PHMSA will take place in order to identify the potential for any related or cascading events. This phase of plan implementation will entail an assessment by DHS/TSA, in conjunction with DOT/PHMSA and other relevant agencies such as DOE, of the level of risk to the pipeline infrastructure. The call will also serve to bring DHS/TSA and DOT/PHMSA together to work jointly on potential recovery measures that may be implemented if preventive measures fail to thwart the incident. All Federal agencies with threat information concerning pipelines will share the information with DHS/TSA and the Federal Bureau of Investigation (FBI).

Figure 1 illustrates the incident continuum along which lead Federal agency actions occur, depending on the incident scope and phase. The three incident phases correspond to the Plan's organization into three main sections. The figure does not include all agencies involved in a pipeline security incident, but represents the Federal agencies with principal roles throughout the three phases: DHS/TSA, DOT/PHMSA, DOE, and FBI. The darker shading in the figure indicates more involvement by the agency at a particular point, and the lighter shading indicates a lessening role.

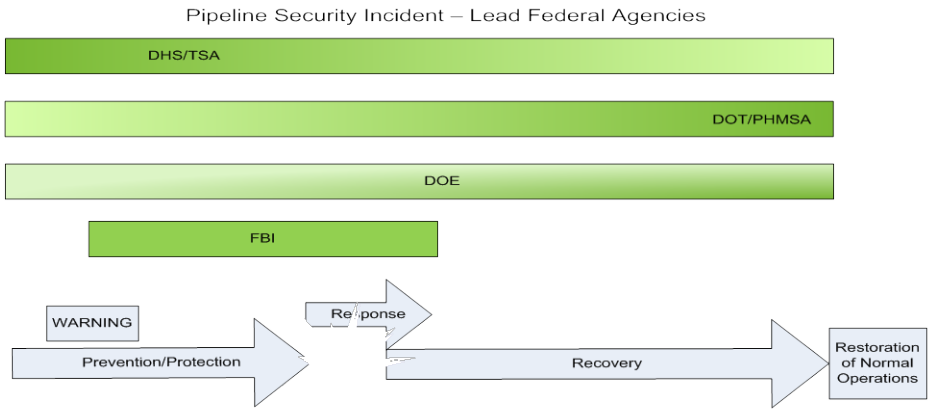

Figure 1 Lead Federal Agency Pipeline Incident Continuum

For the Prevention/Protection phase (refer to Sections 3 and 4), the Plan uses the current pipeline security guidance and safety regulations as the framework within which pipeline operators should be readying for an incident. DHS/TSA is charged with ensuring owner/operators follow security guidelines, while DOT/PHMSA is responsible for enforcing safety regulations. The Prevention/Protection section also defines actions DHS/TSA and DOT/PHMSA can implement during a heightened security threat level to bolster protection from a potential attack. The response and recovery phases of the Plan (refer to Sections 5 and 6, respectively) focus on the actions Federal agencies should take in conjunction with each other to assist owner/operators in restoring services and ensuring product transportation. These two sections identify specific protocols to be followed to facilitate an effective response and recovery.

The objective of the Plan is to establish a comprehensive interagency approach to counter risks and minimize consequences of emergencies involving pipeline infrastructure, specifically focusing on actions the Federal Government can take to assist pipeline protection, response and recovery. The Plan identifies ways in which the Federal Government will provide increased security support to the most critical interstate and intrastate natural gas and hazardous liquid (principally crude oil and refined petroleum products) transmission pipeline infrastructure when threatened, and how the government will work to ensure continued transportation of product following an incident.[2] Pipeline infrastructure covered by this Plan includes transmission lines, distribution lines, intra and interstate lines, terminals, breakout storage, underground gas storage, and onshore liquefied natural gas (LNG) facilities.

The guidance reflected in the Plan is consistent with the organizational concepts described in the National Response Framework (NRF) and NRF Support Annexes, as well as with the National Incident Management System (NIMS) Incident Command System (ICS) procedures. As such, the Plan is scalable and can be implemented to the extent necessary to address a threat or other incident. The Plan recognizes that recovery management involves various levels of government. In general, the affected owner/operator is responsible for pipeline recovery. However, while the majority of pipeline infrastructure assets are privately owned, the Federal Government

[2] The 9/11 Act defines the applicable facilities as "critical facilities of the 100 most critical pipeline operators covered by the September 5, 2002, circular…" P.L. 110-53, § 1557 (b) (2007).

acknowledges that Federal assistance may be required to help the private sector recovery operations.

1.1 Description of Pipeline Threats

The pipeline system is a vital part of the United States (U.S.) transportation and energy supply, with connections to other critical infrastructure such as airports and power plants. Since September 11, 2001, numerous Federal warnings have been issued specifically mentioning pipelines as terrorist targets. Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported, and because pipeline networks are widely dispersed across both remote and urban portions of the country. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.

Pipelines are also susceptible to cyber attacks of their computer control systems. Cyber threats could result from the acts of a terrorist-hacker, or a rogue employee with computer access. The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cyber security protocols. Additionally, attacks on other infrastructure such as regional electricity grids and communication networks could cause a serious disruption in pipeline operations, posing additional risks for all sectors serviced by pipelines, including the military and major commercial installations.

It is impossible to uniformly protect the pipeline system. While it is difficult to predict what method of attack may be utilized, the risks can be calculated in terms of threat, vulnerability, and consequence, and measures can be taken to safeguard the pipeline system. Regardless of the scenario, if the pipeline infrastructure is compromised or shut down, it will require an immediate and coordinated response and recovery effort.

1.2 Implications of Disruption of Pipeline Infrastructure

American oil pipelines carry over 75 percent of the Nation's crude oil and 60 percent of its refined petroleum products.[3] A majority of the Nation's natural gas moves from well to market via pipeline. In addition to oil and natural gas transmission, pipelines are used to transport manufacturing chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

Pipeline disruptions can have an effect that ripples through the economy and, at the most extreme, can impact public health and national security. Minor disruptions may result in increased prices for gasoline, diesel fuel, home heating oil, and natural gas. More prolonged disruptions could manifest themselves as widespread energy shortages and the inability to produce products such as plastics, pharmaceuticals, and many chemicals that rely on oil and natural gas as manufacturing feedstock. In the case of an extreme disruption of pipelines, American transportation and manufacturing could begin to grind to a halt, homes could go cold

[3] Bureau of Transportation Statistics (BTS), "National Transportation Statistics," February 2008.

for lack of natural gas or heating oil, and energy for vital defense use may begin to limit American defense capabilities.

1.3 Planning Assumptions

The Plan is based on the following planning assumptions:

- The Plan is a guidance document for use by decision-makers and their advisors;
- The Plan applies to the entire pipeline industry, including natural gas transmission and distribution and hazardous liquids pipeline infrastructure, including distribution, and interstate and intrastate lines, onshore LNG facilities, terminals, breakout storage, and underground storage areas;
- Pipeline safety and pipeline security measures are intertwined; interagency coordination, including intelligence gathering, analysis, information sharing, and the development of integrated prevention and recovery plans that can be adapted to be responsive to emerging threats is critical to efficient recovery efforts;
- Recovery operations are developed using a risk-based planning method, and security of 100 percent of the pipeline infrastructure cannot be guaranteed;
- Private stakeholders will develop and maintain detailed policies, plans, and procedures consistent with the TSA Pipeline Security Guidelines, to implement a security plan that will include incident management; the Plan will be implemented with awareness of the prevention/protection, response and recovery actions exercised by other Federal agencies and the responsibilities of State, local, and tribal governments;
- Input from private and government stakeholders was considered in the development of the Plan; and
- The Plan will be periodically updated by DHS/TSA, DOT/PHMSA, and other stakeholders to reflect changes in pipeline security threats, technology, and Federal laws and policies.

2 ROLES AND RESPONSIBILITIES

2.1 Federal Role

Various government agencies[4] and private sector entities are involved in pipeline security and recovery efforts. The National Response Framework (NRF) and NRF Support Annexes provide an overview of how Federal, State, local and tribal entities work with the private sector to coordinate and execute functional processes for effective incident management. The Plan recognizes these government entities have responsibility for incident management and recovery efforts in the aftermath of an incident, in accordance with National Incident Management System (NIMS) principles. In order to manage these responsibilities, many of these government agencies have emergency response and recovery plans in place. The goal of the Plan is to describe roles, responsibilities, resources, and relationships to ensure the protection of critical infrastructure and a seamless recovery, and to coordinate actions at the Federal level so the simultaneous implementation of plans does not hinder the protection, response, and recovery phases of an incident.

The discussion below provides a general description of each agency involved in pipeline security and recovery, including their roles, responsibilities, and resources. Federal agencies having a primary role in response or recovery are listed under "key agencies." Other Federal agencies having a limited role are listed under "supporting role." Specific roles of each entity will vary depending on the phase of recovery. The Prevention/Protection, Response, and Recovery sections of the Plan provide Action Charts listing measures key agencies will take during each phase of an incident.

2.2 Federal Role – Key Agencies

Department of Homeland Security (DHS)/Transportation Security Administration (TSA)

DHS/TSA is the lead Federal agency for transportation security, including pipeline security. Specifically, the Pipeline Security Division (PSD) within DHS/TSA's Office of Transportation Sector Network Management (TSNM) is tasked with enhancing the security preparedness of hazardous liquid and natural gas pipeline systems. The PSD works to develop security measures to mitigate risk, monitor compliance with security guidelines, and build and maintain stakeholder relations. In the last five years, security initiatives, in addition to the development of this Plan, include updates to the Pipeline Security Guidelines and enhancements to the Corporate Security Review Program.

As DHS/TSA's mission focuses on increasing security measures to prevent or mitigate the scale of a security incident, actual assets for use in incident response and recovery are minimal. Section 1558 of the 9/11 Act calls for the Plan to identify ways in which the Federal Government can provide increased security support to the most critical interstate and intrastate natural gas and

[4] Within this document, use of the term "agency" when referring to Federal entities is inclusive of executive agencies, departments, and government corporations.

hazardous liquid transmission pipeline infrastructure and operations when under severe security threat levels of alert, or when the security of pipeline infrastructure or operations is specifically threatened. Accordingly, a heightened threat level of alert or specific threat may require DHS/TSA to utilize certain deployable assets. One key DHS/TSA asset includes the Visible Intermodal Prevention and Response (VIPR) teams. VIPR teams are comprised of Federal Air Marshals (FAMs), Federal Security Directors (FSDs), Surface Transportation Security Inspectors (STSIs), Transportation Security Officers (TSOs), Behavior Detection Officers, and Explosives Detection Canine teams. VIPR teams work with local security and law enforcement officials to supplement existing security resources and may be useful in assisting pipeline companies with pre-incident deterrence measures once a threat is identified, as well as post-incident site security. VIPR teams may be deployed at the discretion of the Secretary of Homeland Security or the Assistant Secretary for TSA, and do not require specific conditions for events to trigger deployment. Section 1303 of the 9/11 Act authorizes TSA to use any DHS asset to effectively augment the security of any mode of transportation.

Additionally, DHS/TSA can make use of DHS's Protective Security Advisor (PSA) Program. PSAs are deployable critical infrastructure security specialists that can be used on-scene as Office of Infrastructure Protection (IP) representatives at sites of potential or suspected terrorist incidents. PSAs have a broad set of responsibilities that include maintaining a knowledge of high priority critical infrastructure and key resources (CI/KR) in the State or area they are assigned; maintaining a working relationship with State and local public safety officials, law enforcement, and owners/operators of CI/KR; and coordinating risk mitigation measures that require involvement by the Federal Government. These responsibilities make PSAs uniquely qualified to assist during a pipeline security incident requiring a Federal response effort.

Department of Transportation (DOT)/Pipeline and Hazardous Materials Safety Administration (PHMSA)

DOT regulates the safety of pipelines. Pipeline safety, including pipeline design, construction, operation, maintenance, and incident response is governed by Federal regulations. DOT administers pipeline safety regulations through the Office of Pipeline Safety (OPS), within the Pipeline and Hazardous Materials Safety Administration (PHMSA). DOT/PHMSA's role is to protect people and the environment from the risks inherent in the transportation of hazardous materials and to oversee pipeline repairs and help improve the reliability of systems that deliver energy products and other hazardous materials. In order to carry out this role, DOT/PHMSA, through the OPS, manages the national pipeline safety inspection and enforcement program. OPS oversees the implementation of pipeline operators risk management programs and serves as a DOT liaison with DHS and the Federal Emergency Management Agency (FEMA) on matters involving pipeline safety. Pipeline safety regulations are covered in title 49 of the Code of Federal Regulations 49 CFR), parts 190-199.

The OPS uses a variety of methods to promote compliance with safety standards, including conducting physical inspections of facilities and construction projects, programmatic inspections of management systems, and investigating safety incidents. The OPS also enforces integrity management programs on pipeline segments in high consequence areas, in order to provide for continual evaluation of pipeline conditions. These programs became mandatory in 2001 for most

operators with 500 or more miles of regulated oil pipeline. Similarly, in 2002, the Pipeline Safety Improvement Act established an integrity management program for natural and other gas transmission pipelines.

Like DHS/TSA, DOT/PHMSA can provide minimal assets during a response or recovery. However, DOT has statutory tools that may be useful during a security incident, such as special permits, safety orders, and corrective action orders. DOT/PHMSA also has access to the Regional Emergency Transportation Coordinator (RETCO) Program through S-60. Each RETCO manages regional DOT emergency preparedness and response activities in the assigned region on behalf of the Secretary of Transportation. RETCOs are responsible for coordinating with, and providing assistance to, other Federal agencies and State, local, and tribal governments. DOT/PHMSA has Pipeline Safety Partner Agencies in each State and the District of Columbia. These agencies will be integrated by DOT/PHMSA, as appropriate, throughout all phases of Plan implementation.

Department of Energy (DOE)

In accordance with the National Infrastructure Protection Plan, DOE is the Sector-Specific Agency (SSA) responsible for the energy infrastructure. As such, DOE is responsible for coordinating all activities related to energy infrastructure protection. It executes this responsibility through the Office of Electricity Delivery and Energy Reliability (DOE/OE). DOE/OE is also responsible for Emergency Support Function (ESF) 12, as outlined in the NRF. ESF-12 facilitates the assessment, reporting, and restoration of damaged energy systems and components when activated by DHS/FEMA for energy incidents requiring a coordinated Federal response.

Specific to pipelines, DOE works closely with both DHS/TSA and DOT/PHMSA. During energy emergencies, DOE may monitor flows of throughput and coordinate with Federal agencies and the private sector to assess supply conditions. Other DOE agencies such as the Energy Information Administration, the Office of Fossil Energy (Strategic Petroleum Reserves), and Office of Policy and International Affairs, may become involved in examining the supply impacts of a transportation incident. ESF-12 responders who deploy to the disaster site may also work with the private sector to aid and assist in the restoration and recovery of impacted pipelines. For example, DOT/PHMSA may coordinate with DOE to validate information received from an operator reporting decreased flow before allowing temporary measures to be used to maintain throughput while the problem is corrected.

Federal Bureau of Investigation (FBI)

The FBI is responsible for investigating and prosecuting actual or attempted attacks on critical infrastructure. Any pipeline incident that is or appears to be linked to an intentional criminal act will fall within the jurisdiction of the FBI. The FBI will maintain control of the site until evidence is collected and an investigation is completed. However, the FBI is responsible solely for investigation and does not usually have an incident command function. The FBI will have a key role in assessing and investigating pipeline security threats or events. As a matter of policy, the FBI will respond to <u>all</u> domestic and international leads that may possess a domestic terrorist

nexus, regardless of the source. If DHS/TSA, DOT/PHMSA, or any Federal agency receives threat information, regardless of the source, they must immediately notify the FBI.

2.3 Federal Agencies – Supporting Agencies

Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA)

FEMA is responsible for executing support and planning functions during an incident, in accordance with ESF-5, Emergency Management. If a pipeline event occurs and Federal support is needed, the Secretary of Homeland Security is responsible for implementing the NRF. FEMA within DHS is responsible for carrying out this responsibility, particularly as it pertains to deploying response teams, allocating resources, and working with regional FEMA offices to coordinate the response, as necessary. If a security incident expands in scope and becomes a declared disaster under the Stafford Act, FEMA will have the lead Federal role for the response and recovery.

Department of Homeland Security (DHS)/United States Coast Guard (USCG)

The USCG is the SSA for the Transportation Systems Sector, maritime mode. The USCG has authority to establish procedures, methods, and other requirements to prevent and contain discharges of oil and hazardous substances from vessels and from offshore, pursuant to the Federal Water Pollution Control Act. The USCG has issued prevention regulations for vessels and vessel-related oil transportation facilities, and it shares enforcement duties with the Environmental Protection Agency (EPA). Generally, USCG regulates marine transportation-related facilities, while EPA regulates non-transportation related facilities such as those that produce and process oil and hazardous materials. The USCG and the Minerals Management Service (MMS) are the main points of contact for incidents concerning waterfront and offshore facilities.[5] The USCG has requirements for responding to spills that may result in environmental damage.

Department of Homeland Security (DHS)/Office of Infrastructure Protection (IP)

DHS IP is the lead agency responsible for the coordinated effort to reduce risks to CI/KR posed by acts of terrorism, and for strengthening national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. DHS IP addresses this through the management and support to the Government Coordinating Councils (GCCs) and the Sector Coordinating Councils (SCCs) to facilitate the improvement of security for CI/KR and information sharing. DHS IP conducts voluntary vulnerability assessments and surveys focusing on physical security, security management, security forces, information sharing, and interdependencies. It also provides:

- Information to assist with the protection of CI/KR such as common vulnerability, potential indicators, and protective measures.

[5] For a more detailed discussion of USCG responsibilities for offshore facilities, see the National Strategy for Maritime Security: The Maritime Infrastructure Recovery Plan (April 2006) and the U.S. Customs and Border Protection Joint Protocols for the Expeditious Recovery of Trade.

- Risk mitigation training to reduce risk and assist with closing potential security gaps.
- Geospatial capabilities to support the National Common Operating Picture (COP).
- Information sharing environment (Homeland Security Information Network, Critical Sectors (HSIN-CS)) to facilitate information sharing.
- Development and maintenance of strong relationships with the private sector CI/KR owners and operators, State and local and Federal mission partners.

PSAs serve as the Department's on-site critical infrastructure and vulnerability assessment specialists. They provide a valuable resource to entities seeking to enhance their existing prevention, protection, and response efforts as they relate to critical infrastructure. PSAs are based in local communities, offering a wide range of services to public and private sector Homeland Security partners. They also support incident response and reconstitution efforts during time of emergency. Often they are the first Federal resource available. They provide support to local and State emergency operations centers (EOCs), by working to identify initial impact to infrastructure of concern identity potential cascading effects, assisting in the prioritization of reconstitution efforts, serving as a conduit of information sharing between asset owners/operators, law enforcement personnel and other government officials and DHS, and providing first-hand assessments of local CI/KR status to the incident command and other applicable stakeholders.

National Transportation Safety Board (NTSB)

The NTSB is an independent Federal agency charged by Congress with investigating transportation accidents. The NTSB is required to investigate every civil aviation accident in the United States, and significant accidents in the other modes of transportation including railroad, highway, marine, and pipeline. The NTSB has the discretion to investigate any pipeline accident, but it is required to investigate those involving a fatality, substantial property damage, or significant injury to the environment. An NTSB investigation has priority over any investigation by another department, agency, or instrumentality of the Federal Government.[6] However, the NTSB does not investigate criminal activity, and once it reasonably appears that a transportation accident is the result of a criminal act, the FBI becomes the lead Federal investigative body, with the NTSB providing any requested support. As part of any investigation, the NTSB may issue safety recommendations to help prevent future accidents.

Environmental Protection Agency (EPA)

Under the NRF, the EPA is the coordinating agency for ESF-10, Oil and Hazardous Materials Response Annex. ESF-10 is responsible for coordinating Federal support during an actual or potential discharge or uncontrolled release of oil or hazardous materials. The EPA shares the lead role for ESF-10 with the USCG. Duties under ESF-10 are not limited to response to an oil spill, but also include actions to prepare for potential public health consequences and environmental damage that may be caused by oil or hazardous materials spills. Accordingly, the EPA is authorized to take proactive measures, such as facility inspections and waterway testing to detect and mitigate the risk of product release and contamination. Under the Federal Water

[6] See The National Transportation Safety Board Reauthorization Act of 2006, 49 U.S.C. 1131 (2)(A).

Pollution Control Act, the EPA has jurisdiction for control and inspection of non-transportation related oil facilities. It shares enforcement responsibilities with the USCG, as described earlier in this section. Response to actual oil or hazardous materials spills is generally carried out in accordance with the National Oil and Hazardous Substances Pollution Contingency Plan (NCP), 40 CFR Part 300.

Federal Energy Regulatory Commission (FERC)

The FERC regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects. FERC oversees the certification required to build new interstate gas pipelines. Certificates of public convenience and necessity may have safety or security provisions related to the pipeline route and other factors. Additionally, since 2001, FERC has processed recovery requests from FERC-regulated companies seeking reimbursement for extraordinary expenditures related to securing the pipeline transportation systems. FERC also issued new rules in 2003 allowing owner/operators to immediately start rebuilding pipeline after a terrorist attack, regardless of costs. Previously, such blanket authority had a cost cap and required a 45-day advance notice.

Minerals Management Service (MMS)

The MMS, a bureau in the U.S. Department of the Interior (DOI), is the Federal agency that manages the Nation's natural gas, oil, renewable, and other mineral resources on the Outer Continental Shelf (OCS). MMS works with the USCG on incidents concerning waterfront and offshore facilities. MMS's mission is to manage the ocean energy and mineral resources on the OCS and Federal and Indian mineral revenues to enhance public and trust benefits, promote responsible use, and realize fair value. MMS is currently developing a methodology for assessing the safety of existing pipelines as well as the design and installation of future pipeline systems. MMS' current tactical plan includes developing pipeline standards and guidelines by working with trade associations and assessing the risk and reliability of existing pipeline infrastructure, with a particular focus on hurricane damage, recovery, and damage prevention.

MMS' role is to enhance recovery and minimize disruption of OCS energy production by expediting review and approval of repair procedures for damaged transportation facilities/infrastructure. After an incident, MMS' actions will include prompt review and approval of proposals to resume OCS production through the temporary rerouting of oil and gas production until permanent systems repairs can be made, and to provide engineering and technical support.

Occupational Safety and Health Administration (OSHA)

OSHA is the lead Federal agency responsible for protecting the safety of workers while in the workplace. OSHA regulations cover an array of industries. OSHA regulations pertaining to pipeline safety and the health of pipeline operators are preempted by DOT/OPS regulations, unless an operator is exempt due to certain conditions. However, several OSHA regulations directly impact pipeline construction, maintenance, operations, and emergency response operations. Examples of areas influenced by OSHA regulations include accident prevention

measures, job safety related training, on the job fire protection, accident prevention measures, and construction and excavation operations.

Department of Defense (DOD)

DOD has a broad spectrum of resources that can be utilized during a response or recovery effort. Generally, and in line with Homeland Security Presidential Directive (HSPD) 5, DOD may provide civil support when directed by the President, or when appropriate under the circumstances and the law. DOD's involvement is generally limited to non-law enforcement activities, such as search and rescue efforts and debris removal. DOD is not permitted to engage in law enforcement activities unless permitted by the U.S. Constitution or pursuant to an act of Congress. State-controlled National Guard may conduct law enforcement activities, unless they become federalized. Therefore, DOD's role in a pipeline response and recovery will be limited depending on the scope of the incident.

2.4 Tribal, State, and Local Governments and the Private Sector

Tribal Governments

Tribal governments have individual sovereignty and are therefore responsible for coordinating resources for actual or impending incidents on tribal lands. Like States and localities, when their resources are inadequate or exhausted, tribal governments may seek assistance from neighboring States or the Federal Government.[7] Prior to or during a pipeline security incident, tribal governments will be responsible for taking measures to prevent an incident and coordinating the initial response. The tribal government may be required to communicate emergency information to the tribal community, and amend or suspend certain tribal laws that would otherwise impede an efficient response.

State Governments

The role of a State in recovery will depend on the scope of the security incident. A State may assist the local government by coordinating State resources needed to address the recovery, and may communicate with the public about emergency recovery efforts. Proactively, a State may create orders to be used in certain emergency conditions, and promulgate laws and regulations that will support a recovery. It is beneficial for States to have the legal mechanisms in place allowing for immediate use of mutual aid upon the threat or occurrence of an incident. When State, local, or tribal resources are insufficient or exhausted, a State may take on the role of coordinating requests for Federal assistance and encouraging participation in mutual aid.

Many States have laws and regulations governing the safe operation of pipelines, and enforcing safety regulations is an important State role in terms of preventing accidents and increasing resiliency against security threats. The statutes under which the OPS operates, allow DOT to delegate responsibility for intrastate pipelines to State pipeline safety offices, and provide

[7] As sovereign entities, tribal governments may choose to work directly with the Federal Government when requesting certain types of assistance. However, to obtain Federal assistance through the Stafford Act, a State governor must request a Presidential declaration on behalf of the tribal government.

financial support to these offices through grants-in-aid. These State offices can also act as agents of the Federal Government in administering interstate pipeline safety programs for portions of interstate pipeline falling within the boundaries of the State. For purposes of inspection of these pipelines, the OPS retain enforcement power, whereas States have enforcement authority for regulations applying strictly to intrastate pipelines. The agencies responsible for enforcing the regulations vary among the States, but may include the State Public Utilities Commission, Fire Marshal's Office, or Department of Environmental Protection.

Local Governments

Because of their proximity to the pipeline facilities, local governments will need to be prepared to handle on-site incident response activities. They may be required to provide law enforcement resources to ensure site management control, including incident-specific access, or personnel resources trained to handle fire suppression, and hazardous material spills. Any local laws or regulations that apply to pipeline operations may need to be temporarily waived to address the immediate response effort. Additionally, any laws that may slow the response and recovery may need to be suspended, such as requirements for conditional use permits or site plan amendments before planning commissions, as well as laws limiting the use of certain resources.

Private Sector

The Plan recognizes that the private sector plays a significant role in preventing and recovering from a pipeline security incident. Private sector entities own and operate pipeline infrastructure assets, and are therefore primarily responsible for controlling operations, planning, and initial recovery actions. While the Plan outlines measures the Federal Government can take to facilitate the restoration of pipeline infrastructure, the government will act in concert with private sector efforts. It is anticipated that the private sector will implement recovery and/or continuity of business plans as needed, based on incident information provided by the Federal Government or as required by the situation on the ground. To be as prepared as possible, the Plan advocates that pipeline owners and operators establish appropriate recovery plans or expand on existing continuity of business plans to include recovery planning, as promoted by industry guidance. Additionally, the Plan assumes the pipeline industry is following TSA Pipeline Security Guidelines.

3 PREVENTION/PROTECTION: PIPELINE SECURITY GUIDANCE AND SAFETY REGULATIONS

There are numerous safety regulations, security guidelines, and industry guidance for pipeline operators, adherence to which greatly increases prevention against system safety failures and the ability to protect against a security incident. While DHS/TSA and DOT/PHMSA have distinct missions, any measures to ensure pipeline safety and integrity have a direct bearing on security, and laws and regulations governing pipeline safety are important to understanding the overall pipeline security framework. The pipeline industry also produces voluntary guidelines and industry best practices developed through professional organizations and trade associations as a method of improving pipeline industry operations. Portions of these regulations and guidance documents have an impact on the ability of a pipeline facility to respond and recover from a security incident and are highlighted in Sections 3.1 and 3.2.

3.1 Pipeline Security Guidance

Currently, Federal pipeline security activities rely on voluntary industry compliance with security guidelines and best practices. Section 1557(d) of the 9/11 Act directs DHS/TSA to issue regulations, if the agency determines they are necessary and appropriate. DHS/TSA continues to evaluate the need for pipeline security regulations.

3.1.1 TSA Security Guidance

In 2010, DHS/TSA issued new TSA Pipeline Security Guidelines to replace existing guidance it adopted from DOT's OPS. Prior to issuing the guidelines, DHS/TSA relied on DOT's Pipeline Security Information Circular, issued on September 5, 2002, as the primary Federal guidance for industry security. Complementing this document, and also adopted by DHS/TSA, was the DOT-issued Pipeline Security Contingency Planning Guidance of June 2002. The newly issued guidelines reflect updated security practices and lessons learned.

The guidelines apply to all natural gas and hazardous liquid transmission and natural gas distribution pipelines and to LNG facility operators. Additionally, they apply to pipeline systems that transport materials categorized as toxic inhalation hazards. The purpose of the guidelines is to bring a risk-based approach to the application of security measures throughout the pipeline industry. They provide owner/operators with criteria to assess baseline security risk reduction measures, as well as enhanced measures that should be implemented at critical facilities.

Corporate Security Review Program

TSA's Corporate Security Review Program began in 2003. As part of the program, TSA meets with the most critical pipeline and natural gas distribution operators to review their security plans and visit their facilities. The purpose of the security reviews is to determine whether owner/operators are following the Federal security guidance. The program has uncovered security strengths and inadequacies. The TSA Pipeline Security Guidelines also recommend that owner/operators have an internal Corporate Security Program to document security policies and develop security plans.

Critical Facility Inspection Program

Section 1557 of the 9/11 Act requires TSA to develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline systems. The TSA PSD is collecting critical facility information from the top 100 pipeline systems and beginning inspections of the facilities.

Security Directives

TSA has the authority to enforce immediate protective actions during a heightened threat by issuing security directives. The authority to issue security directives in surface transportation modes was enacted by the Aviation and Transportation Security Act of 2001, Pub. L. 107-71. TSA may issue a security directive to protect transportation security, and can use its authority to compel an industry operator to take certain actions necessary to thwart a security incident when there is specific threat information. When DHS/TSA issues a security directive to a pipeline owner/operator, DOT may issue a complementary safety order, if warranted, requiring certain steps be taken to improve any potentially hazardous condition within a pipeline system or facility.

Chemical Facility Anti-Terrorism Standards

The DHS released an Interim Final Rule on Chemical Facility Anti-Terrorism Standards (CFATS) that imposes comprehensive Federal security regulations for high-risk chemical facilities.[8] The rule establishes risk-based performance standards for the security of the Nation's chemical facilities. CFATS require that covered facilities conduct security vulnerability assessments and prepare and implement security plans according to their particular vulnerability to terrorist attack. The rule covers "any establishment that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department (of Homeland Security)," which may include chemical manufacturing, storage, and distribution facilities, and energy and utilities facilities (unless the facility falls within the regulation of the Marine Transportation Safety Act).[9] The rule does not identify facilities solely on the basis of the chemicals that may be present. Instead, the rule contains a list of certain "chemicals of interest" and corresponding Screening Threshold Quantities (STQs), as an appendix. The list provides a baseline screening threshold to identify facilities that may be subject to compliance.

3.1.2 INDUSTRY GUIDANCE

The pipeline trade associations have been extremely proactive in helping industry enhance pipeline security measures. In particular, the Interstate Natural Gas Association of America (INGAA), the Association of Oil Pipe Lines (AOPL), the American Petroleum Institute (API), and the American Gas Association (AGA) have worked closely with the Federal Government to develop recommended pipeline security guidance. In the aftermath of 9/11, INGAA helped assess industry security programs and began developing common risk-based practices for

[8] See 72 FR 17688 (April 9, 2007).
[9] See 6 CFR § 27.105; see also 6 CFR § 27.110(b) for facilities that are exempt from compliance, even if they contain potentially dangerous chemical substances.

incident deterrence, protection, detection and recovery. The assessments addressed issues such as spare parts exchange, critical parts inventory systems, and security communications with emergency agencies, among other matters. INGAA also worked with Federal agencies, including the DHS/TSA and DOT's OPS, to develop a common government threat notification system. AOPL and API worked together to provide guidance to member companies on how to develop a recommended pipeline security protocol analogous to an existing protocol on managing pipeline integrity.

Together, AGA and INGAA developed *Security Practices Guidelines, Natural Gas Industry Transmission and Distribution* in 2002. The guidelines incorporate a risk-based approach for gas companies to consider when identifying critical facilities and determining appropriate actions. The guidelines offer examples of methods to determine security risks, to implement detection and deterrent practices, and to refine response and recovery practices. API issued *Security Guidelines for the Petroleum Industry* in 2003. The API guidance helps owner/operators identify and analyze the threats and the vulnerabilities facing a facility by conducting a Security Vulnerability Assessment (SVA), and identifies a specific process for conducting SVAs. Together, the API and the AGA/INGAA guidelines incorporate best practices and are used by the pipeline industry to help strengthen and enhance existing security measures.

Beyond written security guidance, oil and natural gas trade associations developed the Oil and Natural Gas Sector Homeland Security Coordination Council in June 2004. The Council serves as a broad industry-wide network to help coordinate ongoing industry initiatives, government partnerships and responsibilities. The Council selects a representative to serve as its chair, and act as the interface to DHS when a sector representative is needed. API serves as the lead trade association for the oil sector, and AGA is the lead for the natural gas sector.

3.2 Pipeline Safety Regulations

The OPS within DOT regulates the design, construction, operation, and maintenance of natural gas and hazardous liquid pipelines. These regulations are codified in 49 CFR Parts 190-199. Several provisions of the regulations specifically address pipeline integrity and risk mitigation measures that make pipelines more resilient. Enforcement of these regulations is important to pipeline security because well-maintained, safe pipelines are more likely to tolerate a physical attack. Pertinent provisions are highlighted in Sections 3.2.1 and 3.2.2.

3.2.1 Mandatory Integrity Management Program

DOT/PHMSA has created mandatory Integrity Management Programs for transmission pipelines carrying liquid or gas that could affect a high consequence area. This requirement is codified in 49 CFR § 195.452 (for liquids) and 49 CFR § 192.901 (for gas). The program requires owner/operators to have written plans that address pipeline risks, baseline assessments of line pipe, identification of pipeline segments that may affect a high consequence area, and a method to ensure continual evaluation of the pipeline to maintain its integrity.

3.2.2 SPECIAL PERMITS, SAFETY ORDERS, AND CORRECTIVE ACTION ORDERS

DOT/PHMSA has statutory authority that may be useful in a security setting. While the regulations were promulgated to specifically address safety issues, safety and security are closely intertwined and provisions related to special permits, safety orders, and corrective action orders are tools DOT/PHMSA may be able to leverage to increase security or facilitate a more efficient response and recovery. While the regulations have been in place for some time, on January 17, 2009, DOT/PHMSA issued a final rule establishing procedures for issuing safety orders and clarifying the procedures governing special permits. The relevant portions of the final rule are codified at 49 CFR § 190.239 and 49 CFR § 191.341, respectively.

Special Permits

Special permits (formerly called waivers) are orders by which DOT/PHMSA waives compliance with one or more Federal pipeline safety regulations. Special permits are issued to individual operators in response to petitions. On an emergency basis, the permits may be issued without requiring notice if the petitioner demonstrates that doing so is necessary to address an actual or impending emergency, is in the public interest, and is consistent with pipeline safety. Normally, the permits must be requested at least 120 days prior to the date they take effect. Special permits are a type of agency order, and set forth specific requirements since the operator is not functioning in accordance with the rule(s) that was waived. Violation of the requirements may subject the operator to civil penalties.

Special permits may be particularly useful in a security incident where waiving specific requirements in context of the emergency may make pipeline access and repair much easier.

Safety Orders

DOT/PHMSA may issue a safety order if there is a hazardous pipeline condition that does not require immediate corrective action. The safety order is designed to address problems that can be corrected over time to avoid failures. If the owner/operator does not consent to the recommendations, the order must cite the condition that poses a specific risk to public safety, property, or the environment. In most cases, issues that might develop and result in the issuance of safety orders are resolved. Safety orders are an important element in guaranteeing the continual assessment of pipeline reliability, which ultimately makes systems more secure.

Corrective Action Order

DOT/PHMSA may issue a corrective action order requiring an owner/operator to rectify a problem that may be hazardous to public safety, property, or the environment. Corrective actions may include suspended use of the facility, physical inspection, testing, repair, or other appropriate action. Corrective action orders are used in situations where specific actions need to be taken to alleviate a hazard and where gradual improvements over a period of time will not suffice. Normally, corrective actions are issued after an owner/operator has been given adequate notice and a hearing, but these requirements may be waived if a situation requires immediate attention and holding a hearing is impracticable.

3.3 Additional Planning Considerations

In addition to security guidance and safety regulations, certain planning considerations should be taken into account by the Federal Government and owner/operators in order to anticipate as many contingencies as possible. While some of these issues are related to on-site incident management and may not immediately impact the Federal Government's coordination effort, they will inevitably come into play depending on how quickly an incident escalates, and it is important that such issues be accounted for in pre-event planning. Some considerations include:

- Identifying major transportation access routes for overland transport (emergency services, equipment) as well as access for law enforcement and private sector personnel needing site access to conduct repairs;
- Ensuring consistent, credible information flow throughout the response and recovery phases;
- Identifying evacuation routes if the site incident is in close proximity to a populated area;
- Identifying any available channels for re-routing pipeline product to maintain flow;
- Having knowledge of the throughput capacity of the affected facility or facilities;
- Understanding the impact of an incident on key infrastructure supplying product to military operations;
- Understanding the impact of an incident on key infrastructure supplying product to major commercial operations; and
- Recognizing the proximity of the incident to waterways, unusually sensitive areas, or other environmental elements needing particular protection.

3.4 Security of Supervisory Control and Data Acquisition (SCADA) Systems

SCADA Systems used by pipeline owners and operators increase efficiency and operational capabilities, but they also increase the exposure of a facility to cyber attacks. Fully recovering from any type of incident is highly dependent on the amount of preparation taken beforehand. For example, incorporating a records retention policy, including creating back-up tapes and preserving activity logs will enhance recovery. The more prepared a company is in advance, the more likely it is that they will be able to reduce losses, restart operations quickly, and identify and take action against perpetrators.

The risk of incidents may be lowered through the establishment of procedures, by training, and by regular assessment activities. Attacks will occur regardless; whether or not they succeed depends on having adequate security controls in place. There is ample guidance for improving the security of SCADA and control systems, including National Institute of Standards and Technology (NIST) SP 800-82, API's Pipeline SCADA Security Document 1164, and the TSA Pipeline Security Guidelines.

A minimum list of appropriate security controls includes:

- Documenting policies and procedures
- Installing physical and logical access controls for cyber assets
- Authenticating authorized users
- Securing network design, including use of firewalls and network segregation
- Ensuring prompt patching or other remedial actions when vulnerabilities in devices or software are found
- Limiting and securing remote and third-party connections
- Allowing only approved devices and computers to connect to the network
- Providing information security training for operators, users, and contractors

Companies should also focus on awareness and information sharing, both within their industries and with outside organizations that focus on information security threats and vulnerabilities. Designated individuals should subscribe to updates and alerts regarding viruses, possible attack attempts, unusual traffic, and other intelligence.

4 PREVENTION/PROTECTION: THREAT DETECTION AND ANALYSIS

The Prevention/Protection section of the Plan focuses on actions DHS/TSA, DOT/PHMSA, and other Federal agencies can take during heightened security threat levels that endanger pipeline infrastructure.

4.1 Operations Centers and Information Sharing

Federal assistance for pre- and post-incident actions requires the timely coordination of information. Numerous organizational elements come into play in order to share and track information among appropriate government and private sector entities. This section describes how these key elements will function for the initial dissemination of information during an increased security threat or other incident.

4.1.1 Overview of Relevant Operations Centers

National Response Center (NRC)

- Is staffed by USCG personnel 24/7
- Is main notification point for oil and hazardous material releases
- Sends initial notification of incident to various Federal, State, and local organizations
- Passes pollution incident reports to pre-designated Federal On-Scene Coordinators, usually officials of the USCG or EPA.
- Receives notification from owner/operators if an incident causes the release of product

Transportation Security Operations Center (TSOC)

- Serves as DHS/TSA Operations Center for security incidents or suspicious activities
- Monitors security-related issues 24/7
- Receives information from intelligence organizations, transportation industry sources, and open sources
- Analyzes intelligence to provide real-time information to decision-makers and to determine changing threat conditions
- Coordinates information with the National Operations Center (NOC) Watch, shares with law enforcement, first responder officials at all levels of government, and industry partners

Critical Incident Management Group (CIMG)[10]

- Is an internal DHS/TSA focus group

[10] A more detailed discussion of the activation and role of the CIMG relative to the TSOC can be found in TSA's Office of Transportation Security Network Management, Pipeline Security Division, Incident Management Plan (February 25, 2009).

- Is activated by TSOC to address security incidents, including pipeline security incidents
- Works with TSOC to facilitate information sharing and interagency incident management coordination, with an emphasis on incident prevention and threat mitigation
- Is co-located with TSOC, and staffed by all modes of DHS/TSA TSNM, including the PSD

Department of Transportation Crisis Management Center (CMC)

- Is located at DOT headquarters and is the central point for transportation response
- Continually monitors national transportation system for all threats and incidents
- Provides information to, and coordinates with, the TSOC and the NOC

National Operations Center (NOC)

- Is an interagency information system bringing together law enforcement, intelligence, emergency response, and private sector reporting
- Includes five elements: the NOC-Watch; NOC National Response Coordination Center (NRCC); NOC-National Infrastructure Coordination Center (NICC); NOC-Intelligence and Analysis (I&A), and the NOC Interagency Planning Element (NOC-Planning)
- Is the primary national hub for situational awareness and operations coordination across the Federal Government for incident management

National Infrastructure Coordination Center (NOC-NICC)

- Is an element of the NOC
- Monitors critical infrastructure and key resources (CI/KR)
- Acts as a coordinating forum during an incident for information sharing across sectors, and may receive information from the private sector

Strategic Information Operations Center (SIOC)

- Is the FBI operations center for all Federal intelligence and law enforcement related to domestic terrorist threats, incidents, or investigations
- Vets and disseminates relevant information to law enforcement
- Maintains direct communication with the NOC

4.1.2 DHS/TSA Interagency Threat Coordination Committee (ITCC)

In recognition of the need to effectively communicate information pertaining to pipeline incidents and to synchronize a response among the relevant Federal agencies, DHS/TSA and DOT/PHMSA established the Interagency Threat Coordination Committee (ITCC). The ITCC is designed to organize and communicate developing threat information among Federal agencies that may have responsibilities during a pipeline incident response. The ITCC will communicate information at the headquarters-level, so the development of Federal action plans can be implemented in a coordinated fashion while avoiding overlap or a duplication of effort. The

ITCC will also work to identify any type of assistance that may be useful to owner/operators and provide subject matter information from Federal experts concerning the threat.

Composition

Standing members of the ITCC include: DHS/TSA PSD, DHS/TSA Office of Intelligence DOT/PHMSA, DOT Office of Intelligence, Security, and Emergency Response, DOE, and the FBI.

Ad hoc members of the ITCC include: the Federal Energy Regulatory Commission (FERC), DHS Office of Infrastructure Protection (IP), and the U.S. Minerals Management Service (MMS). However, the ITCC's composition is fluid, and other government entities with specific expertise and authorities may be included, as necessary. Additionally, if necessary, the State government of the affected area may be included in the ITCC, if it is not already involved in the information sharing process.

Activation

The ITCC will be activated by DHS/TSA PSD. Activation of the ITCC constitutes implementation of this Plan. DHS/TSA PSD will call meetings of the Committee as needed to address escalating threats against pipeline facilities or more general threats in which pipeline facilities may be involved. Meetings may take place in-person, or via teleconference, as is practicable and determined by DHS/TSA PSD. DHS/TSA PSD will determine the location of any in-person meetings of the ITCC. Meeting notes and records of informal communications will be maintained in a case file. The case file will be Sensitive Security Information (SSI), at a minimum, and may be classified by direct or derivative authority, depending on the nature of threat and action information included.

Actions

DHS/TSA will determine the frequency and duration of ITCC meetings, and the activation will continue until the threat is discredited. If an incident ensues, the ITCC will continue to meet and communicate with on-scene units until DHS/TSA determines that the activation should be terminated.

Termination

The Committee will stand down at the direction of DHS/TSA PSD. All communications, emails, and case-related information will be assembled and maintained by DHS/TSA PSD. If National Security Classified Information is involved, the file will be evaluated by Information Security Officials to determine the appropriate level of classification.

4.1.3 FBI Threat Assessment Process

The Plan highlights the FBI's threat assessment process because it is a critical part of credible information sharing, and DHS/TSA relies on the process for determining when to take appropriate actions, such as convening the ITCC, or implementing the Plan. Besides the FBI, threat information may be received by other means, such as through owner/operator reporting.

However, the FBI threat process remains important and any information received by DHS/TSA will be shared with the FBI so it can be analyzed for credibility. Likewise, if the FBI receives intelligence about a pipeline threat, it will share this information with DHS/TSA as it proceeds with the threat analysis process.

The FBI's SIOC operates a watch center on a continuous basis to maintain widespread situational awareness. During a threat or other incident, the SIOC will serve as a conduit for coordination and communication between various law enforcement agencies, other government agencies, and the appropriate FBI personnel and units. The SIOC routinely maintains communications with NOC and Counterterrorism (CT) Watch.

Counterterrorism Watch (CT Watch)

The CT Watch is the FBI's 24-hour global command center for terrorism prevention operations. The CT Watch is located with the National Counterterrorism Center (NCTC), the Nation's primary multi-agency counterterrorism organization.

The CT Watch's primary mission is to direct the immediate response to terrorism threats, incidents, and suspicious activities and provide oversight to FBI response operations. The CT Watch:

- Serves as the focal point for the receipt, preliminary analysis, and immediate assignment for action on all domestic and international terrorism threats with a domestic nexus
- Alerts the FBI Headquarters (HQ) and SIOC, the intelligence community, FBI field offices and the FBI Joint Terrorism Task Forces (NJTTF), among others, of any relevant intelligence
- Maintains oversight over a threat or incident for 24 to 72 hours
- Transfers threat or incident information to a field office or FBI HQ operational unit if an investigation is required
- Transfers information to the Threat Resolution Group for follow up if the threat or incident falls short of the criteria for a formal FBI investigation

CT Watch and Pipeline Threats

Upon notification of a threat to pipelines, or of another pipeline security event, FBI field offices, the CT Watch, or the SIOC will notify the Weapons of Mass Destruction Operations Unit (WMDOU). Within the FBI, responsibility for threats to infrastructure, including pipelines, falls under the Weapons of Mass Destruction (WMD) Directorate. Within minutes of such notification, WMDOU will usually convene a conference call to conduct a threat assessment in an attempt to determine the credibility of the threat, prepare and implement a preliminary investigative plan, and, if necessary, disseminate public safety notifications. The conference call includes other government agencies (OGA) that may have or require information about the threat. If necessary, a formal investigation will take place, and WMDOU will maintain contact with the field office for purposes of investigation oversight and support.

The NOC will obtain information on the status of the FBI response from SIOC or CT Watch reporting. Subsequent dissemination of information to DHS/TSA resides with NOC. It is important to note that in the event of a pipeline incident, DHS/TSA will probably participate in any conference calls and may be invited into the FBI investigation, and NOC will also receive information from DHS/TSA.

Figure 2 illustrates the FBI threat assessment process.

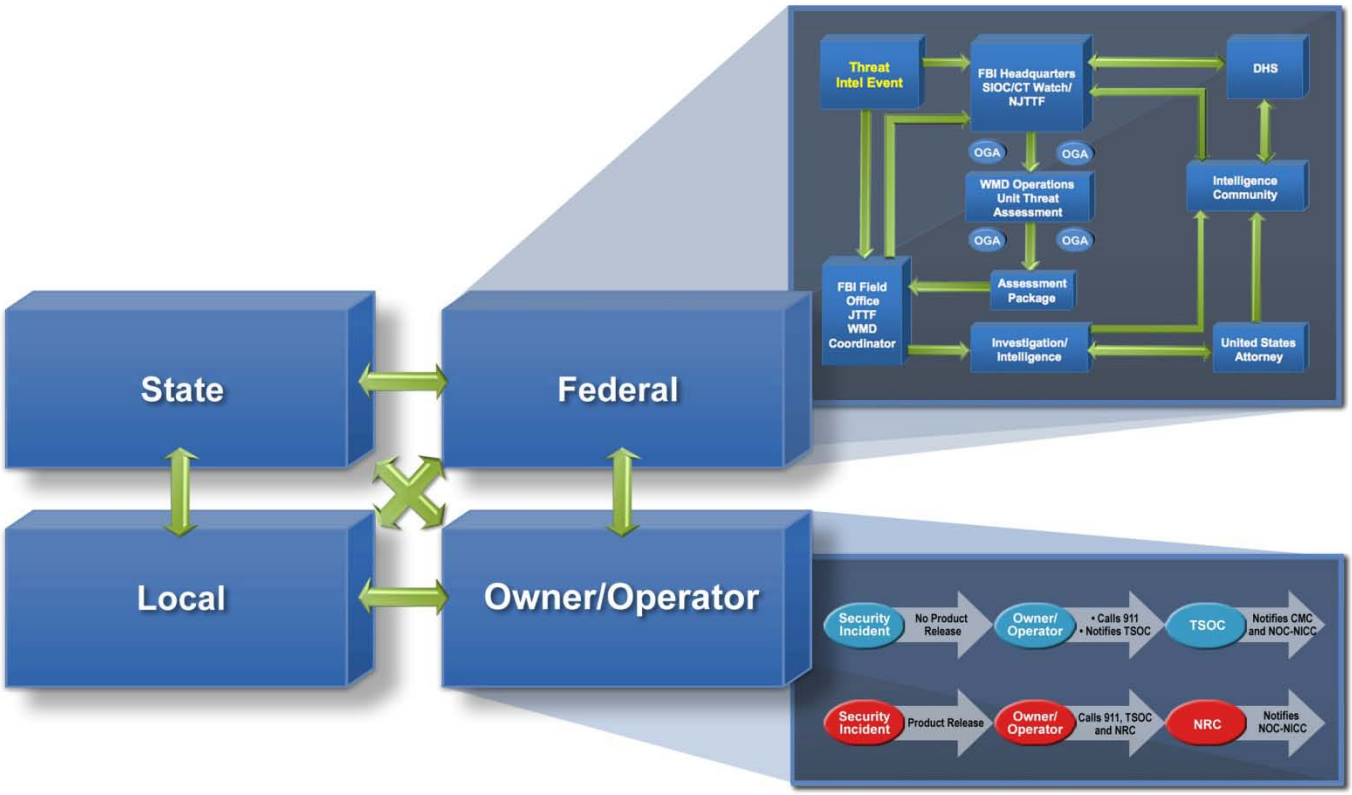

Figure 2 FBI Threat Assessment Process

4.1.4 INTELLIGENCE SHARING

As mentioned in Section 4.1.3, if the FBI receives intelligence about a pipeline threat, it will share this information with DHS/TSA. In some instances, intelligence information is obtained by the FBI through a report from local law enforcement through the National Joint Terrorism Task Force (NJTTF). An individual from DHS/TSA's Office of Intelligence (DHS/TSA OI) is located at the NJTTF, so any information reported to the NJTTF will immediately be sent to DHS/TSA's TSNM by DHS/TSA OI. DHS/TSA will then notify the owner/operator and, if necessary, give protective action recommendations.

If the NOC receives threat information, it will automatically disseminate the information to DHS/TSA and to the NJTTF. The NJTTF is only operational during normal business hours

Monday through Friday, so any threat information reported during off–hours is done via the FBI's SIOC or CT Watch, which report information to the NOC.

4.1.5 Incident Reporting Originating With Owner/Operators

In some instances, information regarding a pipeline security incident will enter the Federal intelligence and threat analysis process when owner/operators report a threat or other security-related event directly to the NRC or TSOC. This reporting process is important in ensuring the information reaches the FBI for comprehensive threat analysis. If the incident does not involve product release, owner/operators should call 911 and TSOC. In instances where there is a product release, owner/operators must notify the NRC. Pursuant to this Plan, owner/operators should also call 911 and then call the NRC if the incident involves product release. Figure 3 illustrates the reporting process for incidents originating with owners/operators.

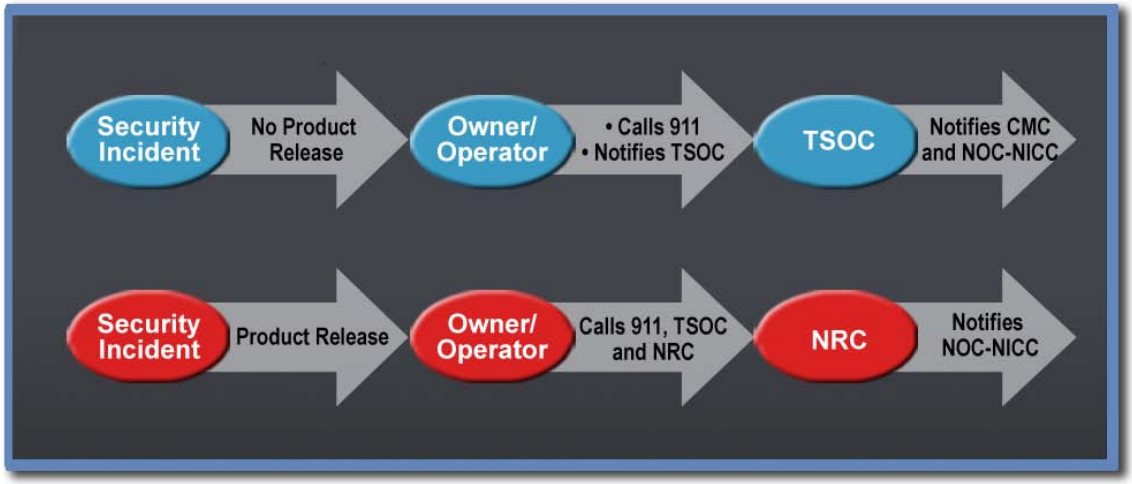

Figure 3 Incident Reporting Originating With Owner/Operator

4.2 Pipeline Incident Operations Coordination

Where appropriate, incident command for pipeline emergencies will be consistent with NIMS, in accordance with HSPD-5. HSPD-5 requires all Federal departments and agencies to adopt NIMS and to use it in their individual incident management programs and activities. This section documents how NIMS will be applied to response and recovery for pipeline emergencies that require a Federal presence.

Overall responsibility for Federal coordination and leadership of the Federal team will reside with the DHS, which is responsible for implementing the NRF and carrying out ESF-5, Emergency Management Responsibilities. Other agencies may have a primary role, even though the overarching coordination role belongs to DHS. DHS will be responsible for ensuring the deployment of any required support assets, coordinating the activities of all on-site Federal assets, and creating the Incident Action Plan (if appropriate) and Situation Reports.

The role of Federal agencies during a pipeline emergency varies with the phase of the emergency. During the prevention/protection phase, DHS/TSA will assume a primary role for Federal activity, with the responsibility to ensure that the activities of other Federal agencies are coordinated and focused through Protective Security Advisors (PSAs). During the response phase, where an incident has occurred, the FBI will begin investigating the incident, but it does not assume an incident command role. On arrival, DOT/PHMSA will lead the pipeline operations sector, branch, or unit depending on the complexity of the incident command system implemented. When response activities are complete and recovery activities take precedence, DOT/PHMSA will continue to work with the owner/operator to facilitate restoration of service.

There can be overlap between the emergency management phases. For example, recovery activities could in principle begin while the response phase is still ongoing. Nevertheless, the agency with incident command responsibility retains that responsibility until a coordinated hand-off occurs.

4.3 Use of Homeland Security Advisory Threat Assessment System for the Pipeline Sector

The Homeland Security Advisory System (HSAS) currently uses color-coded levels to communicate the likelihood or impact of a terrorist attack. The HSAS was established in 2002 by HSPD-3. The HSAS can place certain geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information. From a prevention perspective, the HSAS is a valuable tool for Federal agencies when identifying what protective measures need to be taken against a generalized or specific threat.

Section 1558 of the 9/11 Act requires this Plan to include measures for the Federal Government to provide increased security support to pipeline infrastructure and operations when under severe security threat levels and when there is specific threat information related to pipeline infrastructure. While the law itself requires that these measures apply only to "the most critical interstate and intrastate natural gas and hazardous liquid transmission pipeline infrastructure and operations," Table 1 describes actions that can be taken at each HSAS color-coded level to ensure the increased security of pipeline infrastructure, regardless of its criticality.[11] *The table applies only to the pipeline sub-sector*. The purpose of the measures described in the table is to identify actions the Federal Government will take to reduce security vulnerabilities and risks to pipeline systems and facilities during periods of heightened threat conditions. Implementation and maintenance of progressive levels of protective measures described in the table are dependent on the characteristics of the threat and whether the threat severity escalates. While the lowest HSAS threat level is the Green Condition, the Yellow Condition is considered the level at which normal, day-to-day operations occur.

[11] Specifically, the law uses the definition in §1557 of the 9/11 Act, to define facilities that are included, which refers to "the 100 most critical pipeline operators covered by the September 5, 2002 circular…." IMPLEMENTING RECOMMENDATIONS OF THE 911 COMMISSION ACT, P.L. 110-53, §1557 (2007).

Table 1 HSAS Threat Levels and Corresponding DHS/TSA and DOT/PHMSA Actions

Green: Low Condition **This condition exists when there is a low risk of possible terrorist activity. Green condition is for normal operating conditions. The following actions will be implemented during this condition.**		
Actions	**DHS/TSA**	**DOT/PHMSA**
Steady State	• Status Call between DHS/TSA and DOT/PHMSA	
Blue: Guarded Condition **This condition exists when there is an increased general threat of possible terrorist activity. The following actions will be implemented during this condition.**		
Actions	**DHS/TSA**	**DOT/PHMSA**
Steady State	• Continue any actions occurring during Green Condition • Conduct periodic conference calls	
Yellow: Elevated Condition **This condition exists when there is an elevated risk of terrorist activity. The following actions will be implemented during this condition.**		
Actions	**DHS/TSA**	**DOT/PHMSA**
Current State	• Continue actions occurring during Green and Blue Conditions • Communicate on an as-needed basis • Notify operators of change in threat level	
	• Conduct monthly stakeholder conference calls • Issue weekly security incident reports	• Conduct scheduled inspections of pipeline facilities

Orange: High Condition **This condition exists when there is a high risk of terrorist attacks. The following actions will be implemented during this condition.**		
Actions	**DHS/TSA**	**DOT/PHMSA**
During a general threat (not necessarily pipeline-related)	• Continue any actions occurring during Yellow Condition • Try to determine if events are cascading or coordinated and may impact the pipeline mode	
	• Convene the ITCC, if necessary • Communicate with owner/operators regarding company alert levels and the implementation of corporate security plans* • Interact with stakeholders and other Federal agencies to determine whether the threats could impact pipeline infrastructure	• Participate in ITCC, when initiated by TSA • Coordinate with DOT Office of Intelligence, Security and Emergency Response • Monitor NRC reports
When there is a threat against specific pipeline system(s)	• Convene ITCC and identify appropriate ad-hoc members to be included based on the nature of the threat	• Participate in ITCC as requested by TSA • Coordinate with DOT Office of Intelligence, Security and Emergency Response
	• Interact with stakeholders and other Federal agencies to determine whether the threat is credible	• Work with owner/operators to identify any immediate protective measures to be taken • Coordinate with DOT Office of Intelligence, Security and Emergency Response
Red: Severe Condition **This condition exists when there is a severe risk of terrorist attacks. The following actions will be implemented during this condition.**		
Actions	**DHS/TSA**	**DOT/PHMSA**
During a general threat (not necessarily pipeline-related)	• The actions taken in the Orange Condition will be repeated for a general threat or a specific threat against pipeline infrastructure in the Red Condition	
When there is a threat against specific pipeline system(s)	• Work with owner/operators to identify any immediate protective measures to be taken • Ensure owner/operators have relevant information to institute protective measures • Issue security directives, if necessary	• In coordination with TSA, communicate with owner/operators that may be affected if threat results in an incident

* The Plan assumes that owner/operators are following the recommended security protocols that correspond to each HSAS level as provided in the TSA Pipeline Security Guidelines (2009).

4.3.1 PREVENTION/PROTECTION AGENCY ACTION CHART

Table 2 identifies the actions of key Federal agencies, industry, and the local government in the prevention/protection mission area. This chart also appears in Appendix D, along with the charts for the response and recovery mission areas.

Table 2 Prevention/Protection Action Chart

Prevention/Protection	
DHS Secretary	
Response Role: To execute and support the planning function in accordance with the emergency management Emergency Support Function (ESF)-5	**Actions:** • Work with FEMA to carry out the implementation of the National Response Framework (NRF) if a Federal response to an incident is necessary
DHS/TSA	
Response Role: To enhance the security of hazardous liquid and natural gas pipeline systems by monitoring owner/operator compliance with security standards, building stakeholder relations, and developing security measures to mitigate risk	**Actions:** • Contact counterpart at DOT if threat is security related or if two unknown cause events occur within 24 hours • Consider activation of the ITCC • Interact with stakeholders and other Federal agencies to determine whether the threat is credible • Work with the owner/operator and DOT after a security threat occurs to determine threat credibility • Communicate with owner/operators regarding company alert levels and the implementation of corporate security plans • Coordinate intelligence and security measures and share with other Federal agencies and owner/operators as appropriate
DHS IP	
Response Role: To lead the coordinated national effort to reduce risk to CI/KR posed by acts of terrorism, and strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency	**Actions:** • Manage and support the Government Coordinating Council and Sector Coordinating Council to facilitate the improvement of security of CI/KR and information sharing • Conduct voluntary vulnerability assessments and surveys focusing on physical security, security management, security forces, information sharing, and interdependencies • Provide information to assist with the protection of CI/KR such as common vulnerability, potential indicators, and protective measures

Prevention/Protection	
DOT/PHMSA	
Response Role: To regulate the safety of pipeline design, construction, operation, maintenance, and incident response	**Actions:** • Communicate with owner/operators regarding the personal safety of all employees • Participate in ITCC, if activated • If there is a specific threat, work with the owner/operator and DHS/TSA to determine threat credibility • Coordinate with DOT Office of Intelligence, Security and Emergency Response • Monitor NRC reports • Monitor media reports
DOE	
Response Role: To monitor and assess energy systems in order to identify supply shortages and restore energy throughput to maintain continuous energy supplies	**Actions:** • Monitor media and prepare the daily newsletter, *Energy Assurance Daily*
FBI	
Response Role: To investigate and assess threats	**Actions:** • Issue threat notifications • Domain Awareness – FBI field offices conduct analysis of specific issues in their respective geographic area of responsibility, to include critical infrastructure, and assist with resource and investigative prioritization • Conduct industry outreach • Engage in IT threat awareness, protection, and countermeasures • Continue presence of WMD Coordinator in each field office **Specific Threat Actions**: • Prepare Urgent Report that immediately notifies FBI HQ and all field offices of a threat or event • Conduct threat assessment through WMD Operations Unit, utilizing field office(s), subject matter experts, local/state law enforcement and HAZMAT, and other government agencies, as appropriate • Conduct NJTTF investigation if terrorist nexus suspected; NJTTF is already integrated with local/State law enforcement

This page intentionally left blank.

5 RESPONSE

5.1 Overview of Response Considerations

Response to an incident, as outlined in the NRF, begins at the local level. All response considerations will be managed for an incident as defined by NIMS. For the purposes of this Plan, response refers to actions taken to address an incident that has caused damage to an owner/operator's property, with or without product release.

In this Plan, response to an incident is tiered based on the need for resources to mitigate the situation. The incident will be managed according to the NRF in concert with NIMS. This management will utilize ICS at the incident and the ICS or the Multi-Agency Coordination Systems (MACS) to support command and control through the EOC and/or a multi-agency coordination center (MACC). This system allows for a seamless response and flow across all government levels as well as the private sector. Incident management will begin locally and expand as resource requirements grow and exceed those available. The expansion goes from the local level to the county, State, possibly the regional level, and then the Federal Government. As this expansion occurs, response considerations may become complex in that each action taken by an entity may affect those actions already initiated or planned by another entity involved in the response. This illustrates the importance of good incident command. The dependencies and interdependencies of all the levels of governmental and private sector response must be well managed and coordinated. This Plan will only list those response considerations of Federal Government entities. The Federal Government response must be coordinated with the local incident command system and incident commander. All entities providing response to the incident should consider the following questions, as they manage and coordinate the response:

- Has the Incident Command System been established?
- Who is the incident commander?
- Has an incident action plan been developed?
- What is the communication/notification out?
- What is the communication/notification in?
- What plans, checklists are in place?
- What actions are being taken?
- Priorities? What are the priorities? What assistance is needed?
- Are there any anticipated unmet needs?
- Who is involved?
    - Tied to communications/notifications in?
    - Tied to communications/notifications out?
    - Tied to plans, check lists?

A tiered response for an incident will start with the owner/operator. The owner/operator will notify the local government via the emergency 911 system. This 911 system will begin the

response of the emergency services community to include fire/rescue, law enforcement, emergency medical and hazardous materials, as necessary and appropriate. These services can be provided by local and State governments. Once notification has been made to the 911 system, the owner/operator should call the National Response Center (NRC) (1-800-424-8801), and then notify the Transportation Security Operations Center (TSOC) (866-615-5150), if the incident is security related.

Once local response has been initiated, incident command should be established with an incident commander who manages the event locally. This incident commander will request additional resources as needed. If the incident is security related, consideration should be given to co-locating fire/rescue and law enforcement in the same command post.

As the incident response needs grow, so will the command and control system needed for coordination and facilitation, and support to the incident commander. This may evolve to the activation of a local EOC, the State EOC, and ultimately expanding to the activation of Federal resources and assets. Such expansion will evolve into a managed event following the NRF.

The following foundational documents provide a framework for understanding response:

- National Response Framework (NRF)
- National Incident Management System (NIMS)
  - National Incident Command System
  - Incident Action Plan
- Department of Homeland Security National Security Strategy
- Department of Homeland Security National Infrastructure Protection Plan (NIPP)
- Department of Homeland Security Transportation Systems – Critical Infrastructure and Key Resources (CI/KR) Sector-Specific Plan as input to the NIPP, and specifically Annex F, Pipeline
- Department of Homeland Security and Department of Energy (Energy Sector) – Critical Infrastructure and Key Resources (CI/KR) Sector-Specific Plan as input to the NIPP.

Additionally, all relevant owner/operator, local, State, and Federal Government plans addressing the following:

- Security plans
- Incident response plans
- Emergency operations plans
- Operations and maintenance plans
- Continuity of operations plans (COOP)
- Continuity of business plans
- Recovery plans

This Plan focuses on how DHS/TSA and DOT/PHMSA will work together and coordinate the Federal Government's response to a pipeline incident. As discussed in the Prevention/Protection section, any incident that becomes known by any Federal partners must be reported to DHS/TSA PSD via the TSOC. Once this information is received, the PSD will begin to monitor the incident, initiate its incident management plan, and notify the Federal partners including the members of the Interagency Threat Coordination Committee (ITCC). This Committee will be convened as necessary and per its procedures. Depending on the developments, the deployment of the On-Scene Pipeline Operations Branch may become necessary.

5.1.1 On-Scene Pipeline Operations Branch

Purpose

The purpose of the On-Scene Pipeline Operations Branch is to provide consolidated and integrated Federal pipeline-specific operational command during a multi-agency incident response.

Composition

Standing members of the On-Scene Pipeline Operations Branch include, at a minimum: DOT/PHMSA, and the owner/operator.

Ad hoc members of the On-Scene Pipeline Operations Branch include: DHS/TSA, DHS/IP, MMS, DOE, and FERC. The composition of the On-Scene Pipeline Operations Branch is fluid, and other agencies with specific expertise may be included depending on the facts surrounding the incident.

Activation

DOT/PHMSA inspector(s) will be dispatched to the scene by their Regional Director (RD), in response to incident information from the NRC. The number of inspectors and other personnel dispatched will be determined by the RD, in coordination with DOT HQ staff.

The first arriving DOT/PHMSA inspector will check-in with the Incident Command (IC); present credentials; establish a safe, secure operating location; and notify DOT HQ of contact information.

DHS/TSA may dispatch personnel, including Surface Transportation Security Inspectors, Federal Security Directors (FSDs), Visible Intermodal Prevention and Response (VIPR) teams, and Federal Air Marshals (FAMs).

DHS/TSA personnel should contact the on-scene DOT/PHMSA inspector, and maintain communications with TSOC and DHS/TSA PSD personnel. Whoever arrives first must establish a secure operating location and inform IC and TSOC of contact information.

DHS Infrastructure Protection personnel (*e.g.* Protective Security Advisors) may report to the scene. DHS IP staff should also contact the PHMSA on-scene inspector and maintain

communications with the NICC and TSOC. Whoever arrives first must establish a secure operating location and inform IC, TSOC, and NICC of contact information.

Actions

- Coordinate Federal agency activities with the affected pipeline operator.
- Investigate or cooperate in the investigation of the incident.
- Provide subject matter expertise to the incident command on Federal pipeline safety regulations and procedures.
- Guide or direct safe restoration of pipeline facilities and service.
- Participate in integrated command, representing pipeline safety interests.
- Facilitate needed special permits for pipeline safety, surveying, and construction.
- Coordinate and communicate with the State Pipeline Safety Agency in the affected area.

Termination

This On-Scene Pipeline Operations Branch terminates by consolidating all case files, notes, and evidence from the event; decommissioning the operations site; and traveling to its respective home office.

5.1.2 SITE ACCESS

DHS/TSA PSD and DOT/PHSMA will work within the local ICS to establish, as necessary, badging for owner/operators and other industry response personnel. This badging is specific to an incident, which limits attempts to access various incident sites and establishes legitimacy by identifying individuals with the appropriate credentials. Security and site access is discussed in recent NIMS guidance. Specifically, the guidance states:

> **Security and Access** – *Is the emergency response official permitted access?* Incident/unified command determines the rules that permit a person to have access to resources, sites, and/or systems. Being credentialed does not automatically guarantee access. Security and other personnel should be aware of the rules granting access so that appropriate personnel can be permitted swift access where they are needed. If site-specific "badging" approaches are being used, these badges *should not* be referred to as "credentials."[12]

Badging for access is necessary and any concerns or challenges should be facilitated by DHS/TSA PSD with the local ICS.

[12] NIMS Guideline for the Credentialing of Personnel DRAFT, November 21, 2008.

5.1.3 RESPONSE ACTION CHART

Table 3 identifies actions of key Federal agencies in the response mission area. This chart also appears in Appendix D, along with the charts for the prevention/protection and recovery mission areas.

Table 3 Response Action Chart

Response	
DHS Secretary	
Response Role: To evaluate the need for and if required request a Federal declaration	**Actions:** • Work with DHS/TSA and FEMA to carry out the implementation of the National Response Framework if a Federal response to an incident is necessary
DHS/TSA	
Response Role: To coordinate and collect information, communicate with stakeholders, and provide additional security (if possible)	**Actions:** • Initiate the DHS/TSA Pipeline Security Division (PSD) Incident Management Plan (IMP) • Activate the DHS/TSA Crisis Incident Management Group (CIMG) at Transportation Security Operations Center (TSOC) • Consider activation of the Interagency Threat Coordination Committee (ITCC) as well as possible deployment of the On-Scene Pipeline Operations Branch: – Evaluate the need and possibly send a DHS/TSA representative to augment Federal pipeline representation – Evaluate the need for Federal Air Marshals (FAMs), and the use of Visible Intermodal Prevention & Response (VIPR) teams to assist in providing security at critical locations – Evaluate the need for other Federal agencies, such as, but not limited to: • FEMA • EPA • USCG • FERC • MMS • Provide information to senior leadership via conference calls, emails, and briefings • Collect/coordinate with Federal, State and local law enforcement agencies information received • Evaluate with DOT/PHMSA and DOE which pipelines are most at risk and the consequences of their being taken off line • Disseminate information/recommendations and issue security directive if needed • Notify industry of events through communication channels which may include: Sector Coordinating Councils, Trade Organizations, and direct to owner/operators • Evaluate and respond to industry requests for additional law enforcement resources, evaluate the need for additional security teams (VIPR, FAMs)

Response	
	• DHS/TSA will consider requests from pipeline owner/operators and/or consider assisting coordinating with State/local entities to prioritize resources • Provide factual information concerning the progress of response, recovery and restoration operations from the pipeline operations branch (if present) to incident command and the applicable stakeholders • Prepare congressional information **Resources:** • FAMs and VIPR • Security directive requiring all pipeline operators to implement increased physical security measures at their critical facilities: restricting visitors, checking IDs, installing vehicle barriers, hiring guards, etc.
DOT Secretary/DOT Headquarters	
Response Role: To assess the impact of the event on Transportation Systems	**Actions:** • Operate the DOT Crisis Management Center • Inform DOT Secretary and PHMSA leadership • Activate emergency response team (ERT). The ERT will develop an Executive Summary to communicate the threat level and incident damage and other pertinent information to the Secretary and key decision makers at the affected operating administrations • Coordinate the information flow from other DOT Operating Administrations and the Interagency (Federal, Stateand local levels) • As necessary, operate and staff at NRCC and other field offices under ESF-1 of the National Response Framework

Response	
DOT/PHMSA	
Response Role: To regulate the safety of pipeline design, construction, operation, maintenance, and incident response	**Actions:** • Work closely with DHS/TSA and the ITCC. • Evaluate whether or not to waive certain regulations, provide technical advice to operators, etc • Consult with pipeline operator and if required advocate with State governments for permits to reroute/restore service • Provide factual information concerning the progress of response, recovery, and restoration operations from the pipeline operations branch (if present) to incident command and the applicable stakeholders • Actively communicate with DOE, MMS, and other Federal agencies to assess incident consequences and energy impacts • Advocate for pipeline operator to provide for the expedient/timely restoration of operations. Including facilitating expedient acquisition of special permits and being an advocate for minimizing encumbrances to recovery with other local/State/Federal agencies • Provide technical support to regional offices • Facilitate pipeline operator obtaining emergency special permits; or communicating with other Federal agencies **Resources:** • DOT emergency response mechanism
DOE	
Response Role: To monitor and assess regional, national, and global impacts of incident on energy infrastructure	**Actions:** • Coordinate the flow of information between Federal, State, local agencies and industry to help ensure that accurate information is supplied to energy stakeholders • Prepare Spot Reports for DOE management and DHS and DOT for situational awareness • Prepare Situation Reports for public dissemination and post on public web site • Staff the JFO, NRCC, RRCC, or ITCC that are established to respond to the incidents following an activation (FEMA under ESF-12); DOE coordinates with relevant ESFs and agencies at deployed field locations • Determine whether impact of incident justifies request for emergency release from the Strategic Petroleum Reserve • Determine possible consequences of the incident and assess impact on supply • Conduct due diligence to support an EPA, DOT or DHS/Customs and Border Protection (CBP) decision to issue waivers • Provide information concerning the progress of response, recovery, and restoration operations of a pipeline incident • Advise Federal, State, tribal, and local authorities and industry on priorities for energy restoration, assistance, and supply • Assist Federal, State, tribal, and local authorities with requests for emergency response actions required to meet the Nation's energy demands

Response	
	• Respond to RFIs within specified response time • Issue the Energy Assurance Daily
FBI	
Response Role: Lead law enforcement agency if incident is a terrorist event; conduct investigation	**Actions:** • Coordinate (using the ICS system) with local law enforcement and first responders • Prepare investigative documentation • Interact with pipeline security personnel • Conduct threat assessments. Prepare incident reports and attempt to obtain additional information requested by Supervisory Special Agent • Provide factual information concerning the progress of response, recovery, and restoration operations from the pipeline operations branch (if present) to incident command and the applicable stakeholders **Resources available (if required):** • Hazardous Materials Response Unit for collection of evidence in a hazardous environment • Bomb Data Center and Explosives unit for the post blast investigation • HRT-FBI's enhanced SWAT team • Special Agent Bomb Technicians • WMD Coordinators - Reach back to National Laboratories for additional scientific assistance if needed

6 RECOVERY

6.1 Recovery Protocols

The Federal Government has tools available within several agencies that will facilitate restoration of pipeline operations. Federal capabilities fall into two areas: site- and national-level activities. Site-level activities are focused on expediting and facilitating permitting activities. National-level activities are directed toward ensuring the continued transportation of natural gas and hazardous liquids to essential markets and for essential public health or national defense uses.

6.1.1 SITE-LEVEL RECOVERY SUPPORT

Site-level recovery assistance comes primarily from DOT/PHSMA through four procedures: corrective action orders, consent orders, safety orders, and emergency special permits. DOT/PHMSA tools, while normally used for enforcement, can also be used to facilitate recovery. Corrective action orders (Hazardous Facility Orders), consent orders, and safety orders can be used to facilitate planning and design for repairing facilities. Emergency special permits can be used to expedite otherwise lengthy procedures.

In addition to using Federal statutory authorities as recovery support tools, DOT/PHMSA can facilitate the interaction between Federal, State, and local authorities in facility restoration. For example, DOT community and technical services (CATS) engineers will work as subject matter experts with local permitting and zoning officials in order to help officials understand issues presented by pipeline and facility restoration. By acting as technical resources to State and local officials, DOT engineers can help expedite required State and local permitting actions.

6.1.2 NATIONAL-LEVEL RECOVERY SUPPORT

Incidents that interrupt the transportation of natural gas and hazardous liquids have the potential to have a nationwide impact. The DOE monitors market indicators that may be indicative of potential national impact and initiates corrective action when necessary.

6.1.2.1 Federal and State Actions[13]

Many Federal agencies are involved in the energy sector, including DOE, DHS/TSA, DOT/PHMSA, EPA, MMS, FEMA, FERC, the U.S. DOI, and the U.S. Army Corps of Engineers (ACE). Actions that may be implemented by these agencies are summarized below.

[13] Major portions of this section were taken from "Comparing the Impacts of the 2005 and 2008 Hurricanes on U.S. Energy Infrastructure. Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability. U.S. Department of Energy, available at: ***www.oe.netl.doe.gov/docs/HurricaneComp0508r2.pdf*** .

Monitoring Infrastructure

DOE is the lead agency for Emergency Support Function 12 (ESF-12), which is intended to facilitate the restoration of damaged energy systems and components when activated by the Secretary of Homeland Security for incidents requiring a coordinated Federal response. ESF-12 is an integral part of the larger DOE responsibility of maintaining continuous and reliable energy supplies for the United States through preventive measures and restoration and recovery actions.

ESF-12 collects, evaluates, and shares information on energy system damages and estimates on the impact of energy system outages within affected areas. Additionally, ESF-12 responders provide information concerning the energy restoration process such as projected schedules, percent restored, and geographic progression of restoration.

To achieve these objectives, DOE prepares Emergency Situation Reports, at times twice a day, to provide an official review of the status of energy infrastructure impacted by hurricanes and other natural events deemed to be of national significance. The Situation Reports are distributed widely and posted on the public web site (***http://www.oe.netl.doe.gov/emergency_sit_rpt.aspx***). The Energy Assurance Daily is a newsletter that summarizes the day's major developments and is posted on the public web site as well (***http://www.oe.netl.doe.gov/ead.aspx***).

Facilitating Restoration

DOE provides 24/7 coverage of the ESF-12 desk at regional FEMA headquarters when they are activated during an emergency. DOE has staff dedicated to serve as regional coordinators and has developed an extensive training program to prepare others to step in during emergencies. Staff members are deployed at the National Response Coordination Center (NRCC) in Washington, D.C., Regional Response Coordination Centers (RRCC) in each of the 10 FEMA regions, state emergency operations centers, joint field offices, and other emergency facilities. ESF-12 facilitates the restoration of energy systems through legal authorities. ESF-12 engineers provide technical expertise to the utilities, conduct field assessments, and assist government and private-sector stakeholders in overcoming challenges in restoring the energy system.

Prioritizing Power Restoration

DOE has the authority to invoke Section 202(c) of the Federal Power Act, which gives the Secretary of Energy the authority to determine that an "emergency" exists, and "to require by order such temporary connection of facilities and such generation, delivery, interchange, or transmission of electric energy as in [the Secretary's] judgment will best meet the emergency and serve the public interest."

Strategic Petroleum Reserves (SPR)

The DOE's SPR mission is to diminish the vulnerability of the United States to the harmful effects of petroleum supply disruptions, to meet U.S. obligations under the international energy program, and to maintain the ability to respond to an emergency.

In addition to its authorities with respect to domestic supplies of crude oil, the DOE can seek emergency release of petroleum product reserves in Europe. On September 2, 2005, the United States obtained 60 MMB of petroleum product stocks from the International Energy Agency (IEA), the first such release since the first Iraq war in 1991. IEA member countries hold about 4.1 billion barrels of public and industry oil stocks, of which roughly 1.4 billion barrels are government controlled for emergency purposes. Unlike the SPR, which contains crude oil, the IEA reserves comprise all petroleum products.

6.1.3 WAIVERS

FERC Power Transaction Waivers

On September 4, 2008, FERC granted Entergy two emergency waivers that allowed the company to manage its resources in the wake of Hurricane Gustav. FERC granted the company a waiver of the 1-month minimum term for unit power sales and resales between the Entergy operating companies. FERC also allowed Entergy's operating companies to enter into transactions that included capacity from the Grand Gulf nuclear power plant without advance FERC approval. These waivers were in effect only where an Entergy operating company experienced a significant loss of load as a result of the hurricane, and only until the emergency conditions from the hurricane subsided.

Jones Act Waivers

DOE works with DHS to provide due diligence, *i.e.*, DOE collaborates with other Federal agencies to assess whether an energy emergency exists that would necessitate a temporary waiver. Following Hurricane Katrina, DHS waived the Merchant Marine Act of 1920 (the Jones Act) for certain shipments of crude oil and petroleum products in the Gulf. The Jones Act prohibits foreign built, owned, or flagged vessels from carrying goods between U.S. ports. The waiver, which was effective from September 1 to 19, 2005, allowed large foreign flagged tankers to assist U.S. vessels in the transportation of crude oil and refined products from the Gulf Coast to other parts of the country to alleviate supply problems caused by the shutdown of Gulf refineries and pipelines. On September 26, 2005, after the passage of Hurricane Rita, DHS issued another Jones Act Waiver, effective until October 24, 2005. No Jones Act waivers were requested during the 2008 hurricane season.

EPA Fuel Waivers

Following the hurricanes of 2005 and 2008, EPA waived certain fuel requirements in order to facilitate supply logistics and increase import flexibility. DOE worked closely with the EPA to provide due diligence to facilitate decision-making regarding temporary waiver of certain fuel requirements. In 2005, the EPA granted widespread fuel waivers to states impacted by supply disruptions caused by Hurricanes Katrina and Rita. Thirty States and the District of Columbia, stretching from the east to west coasts and as far north as New England, requested and were granted waivers for gasoline, diesel fuel, or both by the EPA. Seven States - the five Gulf Coast States plus Georgia and Virginia – received fuel waivers for both gasoline and diesel. In addition, the EPA issued a waiver for the entire United States covering the two weeks after Katrina's landfall of the requirement to sell summer gasoline and allowed the early use of higher

volatility wintertime gasoline. Within the same waiver, the EPA also allowed the use of on-highway diesel fuel, which exceeds 500 ppm sulfur content. In 2008, by contrast, fuel waivers were limited primarily to the Gulf Coast and southeastern United States and were granted only for gasoline (with the exception of Texas, which received waivers for both gasoline and diesel).

Driver Hour Waivers

DOE works closely with the DOT/Federal Motor Carrier Safety Administration (FMCSA) during emergencies. When an emergency is declared by a Governor or Federal official, FMCSA regulations automatically exempt motor carriers and drivers providing emergency relief from most of the Federal Motor Carrier Safety Regulations (FMCSRs), including the hours of service limits. Emergency relief is defined as transportation incident to the immediate restoration of essential services (such as electricity, medical care, sewer, water, and telecommunications) or essential supplies (like food and fuel). For large-scale emergencies, the exemption lasts 30 days or the duration of the emergency relief, whichever comes first. As a result of Hurricane Katrina, the exemption had nationwide scope and was extended through October 26, 2005. In 2006, Governors of the States that experienced diesel fuel shortages due to temporary production problems declared their own emergencies, which triggered exemptions from the FMCSRs for drivers of tank trucks carrying diesel fuel to these areas. Because of Hurricane/Tropical Storm Hanna, FMCSA itself declared a regional emergency on September 13, 2008 for six southern States - Alabama, Georgia, Louisiana, Mississippi, North Carolina, and South Carolina. The declaration and driver hour waiver for truckers delivering fuel-related supplies was extended through October 15, 2008.

6.1.4 Responsibilities and Capabilities under the National Response Framework[14]

DOE can provide additional recovery support when activated under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, where DOE has the responsibility under the National Response Framework (NRF) to lead the Energy Emergency Support Function (ESF), ESF-12. DOE will facilitate the restoration of damaged energy systems and components when activated by the Secretary of Homeland Security for incidents requiring a coordinated Federal response. Under DOE leadership, ESF-12 is an integral part of the larger DOE responsibility of maintaining continuous and reliable energy supplies for the United States through preventive measures and restoration and recovery actions. The term "energy" includes producing, refining, transporting, generating, transmitting, conserving, building, distributing, maintaining, and controlling energy systems and system components. All energy systems are considered critical infrastructure. ESF-12 is coordinated through Headquarters DOE. ESF-12 is activated when DHS/FEMA notifies the 24-hour DOE Headquarters Emergency Operations Center.

When activated by DHS/FEMA, ESF-12:

- Provides representatives to the DHS National Operations Center (NOC), Domestic Readiness Group, and National Response Coordination Center (NRCC).

[14] Major portions of this section were extracted from "Overview: ESF and Support Annexes, Coordinating Federal Assistance In Support of the National Response Framework," Department of Homeland Security (January 2008).

- Deploys representatives to the Regional Response Coordination Center (RRCC). The ESF-12 Team Leader at the RRCC coordinates assignments, actions, and other support until the Joint Field Office (JFO) is established and mission-execution responsibilities are transferred to the JFO ESF-12 Team Leader. ESF-12 provides incident-related reports and information to ESF-5 – Emergency Management.
- Deploys personnel as members of incident management teams or the Rapid Needs Assessment Team.
- Deploys personnel to the JFO, if established.

ESF-12 collects, evaluates, and shares information on energy system damage and estimations on the impact of energy system outages within affected areas. Additionally, it provides information concerning the energy restoration process such as projected schedules, percent completion of restoration, and geographic information on the restoration. ESF-12 facilitates the restoration of energy systems through legal authorities and waivers. ESF-12 also provides technical expertise to the utilities, conducts field assessments, and assists government and private-sector stakeholders to overcome challenges in restoring the energy system. ESF-12 provides the appropriate supplemental Federal assistance and resources to enable restoration in a timely manner.

DOE does not act alone when activated as ESF-12 under the Robert T. Stafford Disaster Relief and Emergency Assistance Act. When activated, DOE leads and facilitates any required delivery of Federal support from the Department of Agriculture, Department of Commerce, DOD, DHS, DOI, Department of Labor, Department of State, DOT, EPA, Nuclear Regulatory Commission, and the Tennessee Valley Authority.

Collectively, the primary and support agencies that constitute ESF-12:

- Serve as the focal point within the Federal Government for receipt of information on actual or projected damage to energy supply and distribution systems and requirements for system design and operations, and on procedures for preparedness, restoration, recovery, and mitigation.
- Advise Federal, State, tribal, and local authorities on priorities for energy restoration, assistance, and supply.
- Assist industry, State, tribal, and local authorities with requests for emergency response actions as required to meet the Nation’s energy demands.
- Assist Federal departments and agencies by locating fuel for transportation, communications, emergency operations, and national defense.
- Provide guidance on the conservation and efficient use of energy to Federal, State, tribal, and local governments and to the public.
- Provide assistance to Federal, State, tribal, and local authorities utilizing DHS/FEMA-established communications systems.

Additional Federal support exists in the form of the Terrorism Risk Insurance Program, administered by the Department of the Treasury. While not a direct recovery vehicle, the

Terrorism Risk Insurance Program provides the insurance industry with federally backed reinsurance in order to cover claims arising from terrorist incidents. The Act is intended to allow commercial insurers to provide affordable terrorism coverage to policyholders.

6.2 Recovery Agency Action Chart

Table 4 identifies the actions of key Federal agencies in the recovery mission area. This chart also appears in Appendix D, along with the charts for the prevention/protection and response mission areas.

Table 4 Recovery Action Chart

Recovery	
DHS Secretary	
Recovery Role: To evaluate the need for and if required make a Federal declaration	**Actions:** • Work with DHS/TSA and FEMA to carry out the implementation of the National Response Framework if a Federal response to an incident is necessary • Evaluate the need for Federal assistance
DHS/TSA	
Recovery Role: To enhance the security of hazardous liquid and natural gas pipelines systems by monitoring owner/operator implementation of security standards, building stakeholder relations and developing security measures to mitigate risk.	**Actions:** • Consider the continuation of the activation, or the activation of the ITCC with DOT/PHMSA as well as the use of the On-Scene Pipeline Operations Branch • Determine the need for enhanced security during the recovery phase • Advocate as necessary to ensure access badging for pipeline operators
DOT Secretary/DOT Headquarters	
Recovery Role: Support assistance to owner/operators, and formulate and/or implement any policies necessary to facilitate the recovery	**Actions:** • Coordinate the information flow from other DOT Operating Administrations and the Interagency (Federal, State and Local Levels) • Interface with other agencies and modes *(e.g.* if highway waivers or flight restrictions are involved)

Recovery	
DOT/PHMSA	
Recovery Role: Work with owner/operator to safely restore service to affected facilities.	**Actions:** • Consider the continuation of the activation, or the activation of the ITCC with DHS/TSA as well as the use of the On-Scene Pipeline Operations Branch • Evaluate the need for other Federal agencies, such as, but not limited to: - FEMA - EPA - USCG - FERC - MMS • Consolidate information and utilize regulatory control mechanisms, as appropriate • Provide technical oversight, advice, and guidance to owner/operators • Coordinate recovery activities with State Pipeline Safety Agency, especially in cases where intrastate facilities are affected • Determine need for driver-hour waivers and issue if necessary • Provide technical oversight and guidance • Provide assessment, repair, and restart oversight • Advocate for pipeline operator to provide for the expedient/timely restoration of operations, including facilitating expedient acquisition of special permits and being an advocate for minimizing encumbrances to recovery with other local/State/Federal agencies • Advocate as necessary to ensure access badging for pipeline operators • Evaluate need to relax inspection/reporting requirements from other portions of their system in order for operator to concentrate resources in these emergency areas.
DOE	
Recovery Role: Monitor and assess regional, national, and global impacts of incident on energy infrastructure	**Actions:** DOE is not a regulatory agency, however DOE will: • Coordinate the flow of information among Federal, State, local agencies and industry to help cut down on the burden to industry and to help ensure that correct information is being relayed across all agencies. • Prepare Spot Reports for DOE management that can be shared with DHS and DOT for situational awareness • Prepare Situation Reports for public dissemination and post on public web site • Staff the JFO, NRCC, RRCC, or ITCC that are established to respond to the incidents following activation (FEMA under ESF-12), cooperating with DOT and DHS in those field locations • Determine whether impact of incident justifies request for emergency release from the Strategic Petroleum Reserve • Determine possible consequences of the incident • Conduct due diligence to support an EPA or DOT or DHS/Customs and Border Protection (CBP) decision to issue waivers

Recovery	
	• Provide factual information concerning the progress of response, recovery, and restoration operations from the pipeline operations branch (if present) to incident command and the applicable stakeholders • Advise Federal, State, tribal, and local authorities and industry on priorities for energy restoration, assistance and supply • Assist Federal, State, tribal, and local authorities with requests for emergency response actions required to meet the Nation's energy demands • Provide RFIs within specified response time • Issue Energy Assurance Daily

This page intentionally left blank.

APPENDIX A: ABBREVIATIONS AND ACRONYMS

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ACE	U.S. Army Corps of Engineers
AGA	American Gas Association
AOPL	Association of Oil Pipe Lines
API	American Petroleum Institute
ATSA	Aviation and Transportation Security Act of 2001
BTS	Bureau of Transportation Statistics
CATS	Community and Technical Services
CFATS	Chemical Facility Anti-Terrorism Standards
CI/KR	Critical Infrastructure/Key Resources
CIMG	Critical Incident Management Group
CMC	Crisis Management Center
COP	Common Operating Procedure
CT Watch	Counterterrorism Watch
DHS	Department of Homeland Security
DHS/IP	Department of Homeland Security/Office of Infrastructure Protection
DHS/TSA	Department of Homeland Security/Transportation Security Administration
DHS/TSA PSD	Department of Homeland Security/Transportation Security Administration, Pipeline Security Division
DOD	Department of Defense
DOE	Department of Energy
DOE/OE	Office of Electricity Delivery and Energy Reliability
DOI	Department of the Interior
DOT	Department of Transportation

EIA	Energy Information Administration (DOE)
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FAM	Federal Air Marshal
FBI	Federal Bureau of Investigation
FBI HQ	FBI Headquarters
FEMA	Federal Emergency Management Agency (DHS)
FERC	Federal Energy Regulatory Commission
FIG	Field Investigation Group
FMCSA	Federal Motor Carrier Safety Administration (DOT)
FSD	Federal Security Director
GCC	Government Coordinating Council
HLPSA	Hazardous Liquid Pipeline Safety Act of 1979
HSAS	Homeland Security Advisory System
HSIN-CS	Homeland Security Information Network, Critical Sectors
HSPD	Homeland Security Presidential Directive
I&A	Intelligence and Analysis
IC	Incident Command
ICS	Incident Command System
IEA	International Energy Agency
INGAA	Interstate Natural Gas Association of America
IP	Office of Infrastructure Protection (DHS)
ITCC	Interagency Threat Coordination Committee
JPO	Joint Field Office
LNG	Liquefied Natural Gas

MACC	Multi-agency Coordination Center
MACS	Multi-agency Coordination System
MMS	Minerals Management Service
NCP	National Contingency Plan
NCTC	National Counterterrorism Center
NGPSA	Natural Gas Pipeline Safety Act of 1968
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NJTTF	National Joint Terrorism Task Force
NOC	National Operations Center
NOC-Planning	NOC Interagency Planning Element
NRC	National Response Center
NRCC	National Response Coordination Center
NRF	National Response Framework
NTSB	National Transportation Safety Board
OCS	Outer Continental Shelf
OFA	Other Federal Agencies
OGA	Other Government Agencies
OI	Office of Intelligence (TSA)
OPS	Office of Pipeline Safety (DOT)
OSHA	Occupational Safety and Health Administration
PHMSA	Pipeline and Hazardous Materials Safety Administration (DOT)
PIPES Act	Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006
PSA	Protective Security Advisor

PSD	Pipeline Security Division (TSA)
PSI Act	Pipeline Safety Improvement Act
RD	Regional Director
RETCO	Regional Emergency Transportation Coordinator Program
RRCC	Regional Response Coordination Center
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SIOC	Strategic Information Operations Center
SITREP	Situation Report
SPR	Strategic Petroleum Reserve
SSA	Sector Specific Agency
SSI	Sensitive Security Information
SSP	Sector-Specific Plan
STQ	Standard Threshold Quantity
STSI	Surface Transportation Security Inspector
SVA	Security Vulnerability Assessment
TSA	Transportation Security Administration (DHS)
TSA OI	Transportation Security Administration Office of Intelligence
TSNM	Transportation Sector Network Management (TSA)
TSO	Transportation Security Officer
TSOC	Transportation Security Operations Center
U.S.	United States
USCG	United States Coast Guard
VIPR	Visible Intermodal Prevention and Response
WMD	Weapons of Mass Destruction
WMDOU	Weapons of Mass Destruction Operations Unit

APPENDIX B: DEFINITIONS

Several foundational documents form the basis for the preparedness system discussed in the Pipeline Security and Incident Recovery Protocol Plan (the Plan), including the National Infrastructure Protection Plan (NIPP), the Transportation Systems Critical Infrastructure and Key Resources (CI/KR) Sector-Specific Plan (SPP) as input to the NIPP and specifically Annex F Pipeline, the National Response Framework (NRF), the National Incident Management System (NIMS), and the recently released Federal Emergency Management Agency (FEMA) Comprehensive Preparedness Guide 101 (CPG). Definitions for each mission area (prevention, protection, response, and recovery) differ in the foundational documents. The definition for "incident" also differs slightly among documents.

The Plan identifies an overall approach to pipeline security and recovery referred to as a "preparedness system." The preparedness system addresses four mission areas in the context of security threats and issues in this Plan: Prevention, Protection, Response, and Recovery. These are the mission areas recognized by the Department of Homeland Security (DHS).[15] *However, the Plan condenses the mission areas to three by combining prevention and protection into one area.* Prevention and protection are treated as one phase in the Plan because the measures taken to build readiness and the measures taken to actually implement readiness initiatives are interdependent.

The definitions used in the Plan are a composite taken from some or all of the documents' definitions, resulting in either a blended definition for a given mission area, or a definition taken directly from a single, attributed source**.**

The Plan relies on the following definitions:

Prevention: Measures taken and put in place for the continual assessment and readiness of actions necessary to reduce the risk of threats and vulnerabilities in order to intervene and stop an occurrence, or to mitigate effects. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations, heightened inspections, improved surveillance and security operations, investigations to determine the full nature and source of the threat, and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity. Prevention focuses on reducing the likelihood of threats and consequences.

Protection: Protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures and implementing cyber security measures, among various others.

[15] See FEMA Comprehensive Preparedness Guide (CPG) 101: Developing and Maintaining State, Territorial, Tribal, and Local Government Emergency Plans (March 2009), p. 2-2, available at ***http://www.fema.gov/about/divisions/cpg.shtm*** .

Protective actions may occur before, during, or after an incident and prevent, minimize, or contain the impact of an incident.

Response: Response measures embody the actions taken in the immediate aftermath of an event to save lives, meet basic human needs, and reduce the loss of property and the impact on critical infrastructure and the environment. Response includes the execution of emergency plans and actions to support short-term recovery. Following an event, response operations reduce the physical, psychological, social, and economic effects of an incident. (See NRF, p. 1.) Effective response is related to three phases: prepare, respond, and recover. (See NFR, p. 27.)

Recovery: In the short term, recovery is an extension of the response phase in which basic services and functions are restored. In the long term, recovery is a restoration of both the personal lives of individuals and the livelihood of the community. Recovery can include the development, coordination, and execution of service- and site-restoration plans; reconstitution of government operations and services; programs to provide housing and promote restoration; long-term care and treatment of affected persons; and additional measures for social, political, environmental, and economic restoration. (See NRF, p. 45.)

Incident: An occurrence, natural or manmade, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wild land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war related disasters, public health and medical emergencies, and other occurrences requiring an emergency response. (See NIMS, p.139.)

APPENDIX C: AUTHORITIES

Various Federal statutory authorities and policies provide the basis for federal actions in the context of pipeline infrastructure protection, response, and recovery. These authorities include statutes and regulations pertaining to pipeline safety as well as pipeline security. The Department of Homeland Security/Transportation Security Administration (DHS/TSA) is the lead Federal agency for pipeline security; the Department of Transportation/Pipeline and Hazardous Materials Safety Administration (DOT/PHMSA) is the lead Federal agency for pipeline safety. To understand these complementary roles, it is important to understand the legal authorities directing the agencies' responsibilities, and particularly the transition of security responsibilities from DOT/PHMSA to DHS/TSA. Additionally, several statutes governing Federal action in energy markets and energy regulation are applicable and included below, along with relevant Homeland Security Presidential Directives (HSPDs).

The Natural Gas Pipeline Safety Act of 1968 (Public Law 90-418) and the Hazardous Liquid Pipeline Safety Act of 1979 (P.L. 96-129)

The Natural Gas Pipeline Safety Act ("NGPSA") of 1968 and the Hazardous Liquid Pipeline Safety Act of 1979 ("HLPSA") are the two statutes that provide the framework for the Federal role in pipeline safety. The statutes give DOT the authority to regulate key aspects of interstate pipeline safety. The NGPSA authorizes DOT to regulate the transportation of natural gas and other gases, as well as liquefied natural gas. The HLPSA authorizes DOT to regulate the pipeline transport of hazardous liquids, such as petroleum, crude oil, and anhydrous ammonia. The statutes are codified as 49 U.S.C. Chapter 601.

Aviation and Transportation Security Act of 2001 (Public Law 107-71) and the Homeland Security Act of 2002 (P.L. 107-296)

The Aviation and Transportation Security Act of 2001 (ATSA) established the Transportation Security Administration (TSA) within the Department of Transportation (DOT). ATSA transferred responsibility for security in all modes of transportation to TSA, while the agencies within DOT retained responsibility for transportation safety. ATSA gave TSA, among other things, the power to establish and enforce security measures, conduct threat assessments, and manage intelligence. The Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and transferred TSA from DOT to DHS.

The Pipeline Safety Improvement Act of 2002 (Public Law 109-468)

The Pipeline Safety Improvement Act (PSI Act) was signed into law on December 17, 2002, and reauthorized in 2006. The PSI Act mandates significant changes and new requirements for pipeline safety. The law applies to natural gas and liquid transmission pipeline companies, and requires that each pipeline operator implement an integrity management program similar to the one required for oil pipelines under 49 CFR 195. The integrity management program requires

operators to identify high consequence areas[16], conduct risk analyses of these areas, perform baseline integrity assessments of each pipeline segment, and inspect the entire pipeline system according to prescribed methods. While integrity management is primarily focused on safety, certain elements have links to security.

Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (PIPES Act)

In 2006, the PSI Act was reauthorized as the Pipeline Inspection, Protection, Enforcement, and Safety (PIPES) Act of 2006. The PIPES Act directed DOT/PHMSA to promulgate regulations for the issuance of safety orders if a pipeline facility has a condition that poses a risk to public safety, property, or the environment. The Act allows DOT/PHMSA to order pipeline operators to complete a range of corrective measures. The PIPES Act also clarified DOT/PHMSA's authority to issue emergency and non-emergency waivers of compliance with pipeline safety regulations, referred to as Special Permits.

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

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

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

The Secretaries of Commerce and Energy have been delegated the President's authorities under sections 101(a) and 101(c) of the Defense Production Act (DPA) to require the priority performance of contracts or orders relating to materials (including energy sources), equipment, or services, including transportation, or to issue allocation orders, as necessary or appropriate for the national defense or to maximize domestic energy supplies. DPA section 101(a) permits the priority performance of contracts or orders necessary or appropriate to promote the national defense. "National defense" is defined in DPA section 702(13) to include "emergency preparedness activities conducted pursuant to title VI of the Robert T. Stafford Disaster Relief

[16] High Consequence Area means: a commercially navigable waterway, a high population area (50,000 or more people with density of 1,000 people per square mile), any other populated area as defined by Census Bureau, or an Unusually Sensitive Area (USA). 49 CFR §§ 195.450, 195.6.

and Emergency Act and critical infrastructure protection and assurance." The Secretary of Energy has been delegated (Executive Orders 12919 and 11790) the DPA section 101(a) authority with respect to all forms of energy. The Secretary of Commerce has been delegated (Executive Order 12919) the section 101(a) authority with respect to most materials, equipment, and services relevant to repair of damaged energy facilities. Section 101(c) of the DPA authorizes contract priority ratings relating to contracts for materials (including energy sources), equipment, or services in order to maximize domestic energy supplies, if the Secretaries of Commerce and Energy, exercising their authorities delegated by Executive Order 12919, make certain findings with respect to the need for the material, equipment, or services for the exploration, production, refining, transportation, or conservation of energy supplies**.**

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

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

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

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

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

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

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

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

HSPD-3, Homeland Security Advisory System (March 2002)

Homeland Security Presidential Directive-3 (HSPD-3) mandates the creation of an alert system for disseminating information regarding the risk of terrorist acts to federal, state, and local authorities, and the public. It also includes the requirement for a corresponding set of protective measures for Federal, State, and local governments to be implemented, depending on the threat condition. Such a system provides warnings in the form of a set of graduated threat conditions that are elevated as the risk of the threat increases. For each threat condition, Federal departments and agencies are required to implement a corresponding set of protective measures.

HSPD-5, Management of Domestic Incidents (February 2003)

Homeland Security Presidential Directive-5 (HSPD-5) establishes a national approach to domestic incident management that ensures effective coordination among all levels of government and between the government and the private sector. HSPD-5 requires the Secretary of Homeland Security to develop and administer the National Incident Management System (NIMS) and the National Response Framework (NRF). Federal departments and agencies are required to adopt NIMS and the NRF. Accordingly, the Plan is written consistent with these concepts**.**

HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

Homeland Security Presidential Directive-7 (HSPD-7) establishes a national policy for identifying, prioritizing, and protecting key critical infrastructure. Under HSPD-7, DHS has the

lead role for coordinating protection initiatives for pipeline infrastructure. HSPD-7 further requires that DHS implement an overarching approach for integrating the numerous critical infrastructure protection initiatives. The National Infrastructure Protection Plan (NIPP) was created to meet this requirement.

HSPD-8, National Preparedness (December 2003)

Homeland Security Presidential Directive-8 (HSPD-8) establishes policies to strengthen the preparedness of the United States to prevent, protect, respond to, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies by: requiring a national domestic all-hazards preparedness goal; establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments; and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities. This directive mandates the development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all entities involved adhere to the same standards. The directive calls for an inventory of Federal response capabilities and refines the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004)

Homeland Security Presidential Directive-12 (HSPD-12) establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors to enhance security, increase governmental efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard Publication**.**

National Infrastructure Protection Plan (NIPP) and Sector-Specific Plan (SSP)

The National Infrastructure Protection Plan (NIPP) is designed to coordinate the Nation's critical infrastructure and key resource protection initiatives. The NIPP designates DHS/TSA as the lead agency for the transportation sector, which includes pipelines, and requires that each sector have a sector-specific plan. DHS/TSA fulfilled this requirement with the creation of the Transportation Systems Sector-Specific Plan and Pipeline Modal Annex (SSP) in May 2007. The SSP recognizes DHS/TSA's lead role with respect to pipeline security, as well as the role of other Federal agencies and industry stakeholders**.**