Order Code RL31391

Pipeline Security: Industry and Federal Efforts and Associated Legislation

April 26, 2002

Paul F. Rothberg
Specialist in Science and Technology
Resources, Science, and Industry Division

Pipeline Security: Industry and Federal Efforts and Associated Legislation

Summary

Congressional interest in enhancing the security of U.S. pipelines stems from the essential role that this infrastructure plays in the delivery of crude oil, natural gas, and refined petroleum products, as well as associated safety and pollution risks. The pipelines that deliver these commodities often cross heavily populated or environmentally sensitive areas. About 272,000 miles of pipeline in the natural gas transmission system feed a 1.2 million-mile distribution system. Through a network of some 200,000 miles, oil pipelines carry roughly 68% of the petroleum shipped in the United States. To address security concerns, several bills have been considered. H.R. 3609 seeks to strengthen federal regulations regarding the security of this infrastructure. S. 517 , as amended, includes the previously passed Senate pipeline safety bill (S. 235) plus a new provision seeking a balance between the release of information to meet "community right to know" interests and the withholding of security-sensitive data about pipeline vulnerabilities. H.R. 3555 authorizes funds to assess pipeline vulnerability and to demonstrate good security practices. H.R. 3929 authorizes $20 million for each of FY2002 through FY2006 for a cooperative federal program for research, development, and demonstrations related to pipeline security.

Both the private and public sectors have taken steps to enhance the security of the pipeline infrastructure. Since September 11, 2001, many pipeline companies are: operating at a much higher state of alert, evaluating the location of control centers, limiting access to important equipment, increasing security at plant gates, reexamining the background of employees in key positions, posting guards at certain vulnerable facilities to help deter a terrorist attack, and improving communications. In addition to assessing vulnerability and identifying best security practices, the Office of Pipeline Safety (OPS) in the Department of Transportation (DOT) serves as the major contact point within the federal government for many pipeline security concerns.

The Interstate Natural Gas Association of America reports that there is no specific threat to the gas-carrying infrastructure in the United States. The Association of Oil Pipe Lines states that oil pipelines are operating under normal output levels (conditions) and that no special security risks have been detected. But, at any time, the risks faced by either oil or gas pipelines companies can change. The OPS in DOT has warned that critical pipeline facilities, such as control centers, pump and compressor stations, as well as storage facilities may be targets for terrorist attacks. OPS assessments indicated that many of these facilities need to be better protected.

In assessing risk, pipeline releases caused by corrosion, operator error, and third-party damage are much more prevalent than intentional actions seeking to damage pipelines. Nevertheless, this infrastructure is so extensive that it will never be possible to prevent an attack on the network. In fact, there may be no warning before a catastrophic event takes place. If an attack did occur, the extent of damage that might result, and how fast service might be restored, would depend on the circumstances of the attack and the location and nature of the facility affected.

Contents

Pipeline Security: Industry and Federal Efforts and Associated Legislation

Introduction

In response to the terrorists attacks of September 11, 2001, much attention is focused on ways to improve national security, with particular emphasis being placed on critical infrastructure, including oil and gas pipeline systems. The security of pipelines is especially important because of their essential role in the delivery of crude oil, natural gas, and numerous products of commerce, e.g., refined products made from petroleum. This report first discusses efforts of the natural gas transmission and distribution companies to enhance the security of their pipeline infrastructure. As discussed below, these efforts often include: definition of the threat, development of a notification system and security plan, deterrence of a threat (protection and monitoring of physical infrastructure and control systems), response to and recovery from an incident, and coordination with governmental activities.

In addition to industry efforts, several federal agencies are concerned about the security of pipeline systems, including the new Transportation Security Administration (TSA) and the Office of Pipeline Safety (OPS) within the Department of Transportation (DOT), the Department of Energy, and the Federal Energy Regulatory Commission. Because the OPS is the primary point of contact within the federal government for the broad range of activities pertaining to pipeline security and because this agency exerts a substantial regulatory role over this industry, this report focuses on its activities.

Government and industry efforts are discussed separately in this report, but the security of pipeline systems is being strengthened through the combined efforts of the involved parties. An analysis of the adequacy of ongoing efforts to increase pipeline security is beyond the scope of this report. Such an assessment would be difficult to conduct given the sensitivity of security measures, as well as the unpredictability of terrorist actions.

As evidenced by several hearings and bills, many in Congress are interested in efforts underway to promote the security of the pipeline infrastructure. Legislation intended to strengthen pipeline security is summarized in the last section.

Efforts and Views of the Natural Gas Transmission and Distribution Companies

About 272,000 miles of pipeline infrastructure in the natural gas transmission system feed a 1.2 million-mile distribution system to supply more than 63 million homes and businesses throughout the Nation. Given its size and location, the task of

promoting the security of this complex infrastructure is challenging. Nevertheless, the Interstate Natural Gas Association of America (INGAA) reports that pipeline operators are unaware of any specific threat to this infrastructure in the United States.[1] But, at any time, this situation can change. According to the INGAA, pipeline companies are on a heightened state of alert and are working with appropriate law enforcement agencies to ensure the continued safe operation of their facilities.[2]

Especially in light of the events of September 11, 2001, the natural gas companies report that they have committed significant resources to implement security procedures at their critical facilities. Many in the gas pipeline industry are approaching security from a systems point of view, focusing on protection of assets, deterrence of attacks, response to threats or events, and recovery from a release. For example, starting with a risk-based approach that assesses consequences of a release, potential threats specified by the FBI and an assessment of their possible outcomes, and other factors, many companies have been identifying critical areas of their pipeline facilities. According to the American Gas Association (AGA), actions to either maintain or enhance security at such facilities include: strengthening emergency, contingency, and business continuity plans; increasing liaison with law enforcement; increasing the monitoring of visitors and vehicles on property; monitoring pipeline flows and pressure on a 24/7 basis; increasing employee awareness to security concerns; and deploying additional security personnel.[3] Also, multiple redundancies along the delivery system can provide operators flexibility to redirect or shut down product flow, using compressors or valves to control flow, pressure, and direction.

During this period of uncertainty, AGA has been communicating alerts to its members as they receive them from FBI, DOT, or Department of Energy. To improve communications over the long-term, AGA has recommended other approaches, such as receiving direct alerts from the FBI or using the Energy Information and Sharing Analysis Center. (This center consists of a secure database and information gathering and distribution facilities that provide information on physical or information security threats, incidents, and solutions exclusively for professionals in the energy industries.)

Natural gas companies have much experience in preparing for and responding to catastrophic events that affect their ability to deliver service to their customers. They emphasize their safety and emergency response plans already in place for dealing with more "commonplace" threats to service, e.g., earthquakes, excavators, or floods.[4] On the one hand, this experience in dealing with sudden releases provides some degree of assurance to those concerned about sudden disruptions that might occur from a terrorists attack. Then again, the size and nature of the damage that

---

[1] See INGA web site at:
http://www.ingaa.org/main/index.php?page=main

[2]Ibid.

[3]American Gas Association. *Natural Gas Distribution Industry Critical Infrastructure Security*. 2002, and American Gas Association. *Natural Gas Infrastructure Security– Frequently Asked Questions*. November 12, 2001.

[4] See American Gas Association. *Natural Gas infrastructure Security– Frequently Asked Questions*.

might be inflicted by such an attack would depend on the specific circumstances of the attack and the location and nature of the facility affected.

In testimony before a subcommittee of the House Transportation and Infrastructure Committee, a spokesman for the INGAA pointed out other efforts underway. Industry has determined that it can be more prepared to respond to a terrorist incident if it formalizes cooperation among companies on the exchange of spare parts. Also, industry is assessing the need for separate regional inventory systems of critical items, and is reviewing the effectiveness of communications concerning security with the public, local emergency planning committees, and others.[5]

The gas transmission and distribution industry is proposing different levels of threat alerts and specifying voluntary action guidelines that could be implemented at critical facilities in response to each level of perceived threat. The industry is seeking a common understanding with the federal government on the degree of security preparedness and the nature of responses that will be expected from natural gas utilities. Both industry and government are working on guidelines to determine what is a critical pipeline facility. Commonly adopted definitions of threat levels and other key security parameters would be intended to promote clearer communications among government and industry. Many in the gas pipeline industry are urging federal governmental agencies to adopt and use common definitions. They hope that these definitions and benchmarks for security action would be adopted voluntarily and appropriately applied to the unique operating conditions or location of each system. AGA maintains that each utility is in the best position to determine the threats to its system and the responses it should take. Many in industry do not want federally-set regulations for preparedness, but favor voluntary guidelines.[6]

Other industry recommendations include designation of a single government agency for oversight on critical infrastructure security; strengthening of their ability to protect their infrastructure and rapidly repair and recover effectively from the damage that might be caused by a terrorists attack; and passage of legislation better protecting security-sensitive information about pipelines.

Efforts and Views of the Oil Pipeline Companies

Through a network of some 200,000 miles of infrastructure, oil pipelines carry roughly 68% of the petroleum shipped in the United States. This infrastructure, which delivers over 14 billion barrels of petroleum each year, contributes to the U.S. economy, quality of life, and national security.[7] Many military bases, industrial users (e.g., power plants and chemical plants), and airports receive petroleum products directly from pipelines. This infrastructure is frequently used to transport petroleum

---

[5]Statement of William J. Haener. On Behalf of The Interstate Natural Gas Association of America (INGAA) before the Subcommittee on Highways and Transit, House Transportation and Infrastructure. February 13, 2002.

[6] Based on discussion with staff of the AGA, 2002.

[7] Allegro Energy Group. *How Pipelines Make the Oil Market Work–Their Networks, Operation, and Regulation*. December 2001. p. 2.

between regions–often from supply sites to consuming sites. To promote successful pipeline operations, safety, environmental protection, and security need to be closely integrated. To further this objective, oil pipeline companies use many different means, including: aerial surveillance at low altitude and driving patrols to monitor activities close to or along the pipeline rights-of way, redundant safety systems (telecommunications, distributed control), restricting access to facilities, testing and activation of backup control centers, and reevaluation and practicing of spill response plans.

Since September 11, 2001, various oil pipeline companies have taken measures to enhance the security of their operations. Working with government and others, these companies state that they have been assessing the vulnerability of their systems and taking such actions as: operating at a much higher state of alert, increasing employee awareness related to security, evaluating the location of control centers, limiting access to important equipment, increasing security at plant gates, reexamining the background of employees in key positions, hardening (increasing the security or survivability of) control rooms, evaluating backup control centers and their physical relationship to operating centers, posting guards at certain vulnerable facilities to help deter a terrorist attack, and improving communications with law enforcement and security-related officials.[8] Most companies continue to operate in a state of heightened security.

In addition, the Association of Oil Pipe Lines (AOPL) and the American Petroleum Institute (API), working together, have issued to member companies standardized levels of alert with specific recommended actions to enhance security at each threat level. (These recommendations are somewhat analogous to the concepts recommended by the gas pipeline industry, which were described previously.) AOPL and API have also drafted a guidance document on how to develop a pipeline security plan, which is now being reviewed by their members. To a large extent, the guidelines are analogous to an existing standard on managing pipeline integrity that has been accepted and is being integrated into oil pipeline company operating practices. Some companies have stated that they would add security-oriented measures into company pipeline integrity management plans.[9] Like the gas pipeline industry, the oil pipeline industry is also trying to reconcile its levels of security threat and associated security measures to be taken at each level of threat with the levels of security threat issued by the Office of Homeland Security.

The AOPL states that all pipelines are operating under normal output levels (conditions) and that no special security risks have been detected.[10] Despite substantial private and public efforts to promote security, there will always remain certain vulnerabilities, especially when one considers the location and extent of the oil pipeline network.[11] However, it is widely recognized that the pipeline systems are so

---

[8] Based on discussions with the Association of Oil Pipe Lines, 2002.

[9] Ibid.

[10] See the Association of Oil Pipe Lines website at:

http://www.aopl.org/news/Pipeline%20Security%20statement18sep01.pdf

[11] For example, in October 2001, someone fired a rifle repeatedly at a segment of the Alaskan

(continued...)

extensive that it will never be possible to prevent an attack on the entire system. In fact, there may be no warning before a catastrophic event takes place. But, special emphasis can be placed on strengthening the security of especially vulnerable areas, such as control centers, junctions, or storage (tankage) systems.

The challenge is to harden (i.e., to enhance the security of) the pipeline system and ensure adequate surveillance and monitoring. The main response is to recover quickly from any interruption and limit the scope and nature of any release.[12] In that sense, the response to terrorist attacks may be similar to that taken to respond to a more conventional release, with two major exceptions. Any terrorist attack could result in the area surrounding the incident being declared a crime scene and potentially limiting a company's ability to repair the pipeline and restore service. If a radioactive agent, a nuclear explosive, a bomb contaminated with nuclear materials or a biochemical agent is used to rupture a pipeline, even the immediate response (stopping the rupture, clean up, restoration) would be significantly more complicated and much more difficult.

In addition to supporting H.R. 3609 (discussed below), AOPL favors governmental intervention that would facilitate the ability of oil pipeline companies to rapidly restore oil pipeline service from an interruption that might be caused by a terrorist attack. Thus, the AOPL favors a provision in federal law that would provide for access to land for constructing an alternative pipeline segment if a critical pipeline segment is damaged due to a terrorist attack. Elaborating on this point a spokesman for the AOPL and the API stated:

> With regard to recovery, we believe there is a particular need for the government to review its emergency authorities and develop workable plans for emergency access to alternate rights of way around attack sites. After a successful terrorist attack, the attack site may be inaccessible to the pipeline operator for some time because of contamination or because it is a crime scene. Yet the public interest will be the earliest resumption of service possible. Without emergency re-routing authority, service resumption may be unreasonably delayed.[13]

On the other hand, there are formal state, local, and federal procedures for the granting of new pipelines rights-of-way and other approvals. Depending on the location, extent, and duration of the re-routing, citizen opposition could be substantial.

(...continued)
oil pipeline system, ultimately penetrating the pipeline in one location. This created a substantial oil spill requiring the shut-down of the system for several days.

[12] Personal communication with staff of Association of Oil Pipe Lines, 2002.

[13]Statement of William H. Shea. On Behalf of the Association of Oil Pipe Lines and the American Petroleum Institute. Before the Subcommittee on Highways and Transit. U. S. House Committee Transportation and Infrastructure. February 13, 2002.

Efforts of the Office of Pipeline Safety (OPS)

The fundamental functions of the OPS include promoting the safety of pipeline systems and conducting activities intended to reduce environmental impacts caused by pipeline releases. Through its enforcement of the traditional pipeline safety regulations, oversight and promotion of integrity management plans, sponsored drills of oil spill response plans, and various outreach activities with industry, OPS seeks to reduce the probability of a pipeline release, and improve emergency response in the event of a release. As discussed below, these functions are intertwined with promoting the security of pipeline systems.

There are many OPS regulations that have important implications for promoting security and improving responses to releases, whether such releases occur from natural causes, by excavators, or from a malicious action. For example, OPS requires specified pipeline operators to prepare and follow for each pipeline a manual of written procedures for emergency response, (see 49 Code of Federal Regulations (CFR) 192.605). In 49 CFR 192.615 OPS requires specified operators to establish written procedures to minimize the hazards from a gas pipeline emergency, including procedures for establishing and maintaining communications with governmental emergency response and other public officials. Also, OPS specifies detailed security standards for liquefied natural gas facilities, (see 49 CFR Subpart J of Part 193). Those regulations pertain to protective enclosures, security communications, and security lighting and monitoring. In addition, specified oil pipeline companies are required to prepare oil spill contingency plans intended to promote effective response to releases. OPS approves the spill response plans for specified hazardous liquids operators.[14] Federal regulations also specify that certain releases or spills from liquid and gas pipelines must be reported to DOT's National Response Center, (see 49 CFR 195.52 and 191).

Especially during the last 5 years, OPS has conducted many activities that promote industry's implementation of integrity management programs, which have particular implications for promoting pipeline security. OPS has issued new safety standards requiring the implementation of such programs, which must provide for continual assessment and evaluation of certain pipeline segments, inspection or testing, data analysis, and followup repair as well as preventive or mitigative actions on pipeline segments transporting hazardous liquids that are located in or could affect high consequence areas.[15] If an operator knows or it is reasonable to anticipate that there is a threat due to a terrorist activity, the operator must consider that risk in developing its integrity management program, according to OPS. That agency is expected to propose comparable regulations for gas pipeline segments.

In response to the September 11, 2001 attacks and other concerns, OPS issued several emergency bulletins to numerous oil and gas pipeline companies to

---

[14]Those entities covered under the federal pipeline safety regulations should refer directly to the CFR and should not depend upon the summary presented above.

[15]DOT. RSPA. *Pipeline Safety. Pipeline Integrity Management in High Consequence Areas (Hazardous Liquid Operators with 500 or More Miles of Pipeline*). Federal Register. Dec. 1. 2000: 75378. High consequence areas include populated areas, commercially navigable waters, and unusually sensitive areas, including drinking water or ecological resource areas.

communicate the need for a heightened state of alert in the pipeline industry. According to a DOT official, "OPS personnel made immediate and individual telephone contact with all major pipeline operators to ensure that communication was open and viable between our offices and that they understood and adhered to the security issues. Additionally, OPS personnel contacted all of the State pipeline safety programs to provide them with security information."[16] Soon after September 11, 2001, the OPS, because of national security concerns, removed from its web site detailed maps of the country's pipeline infrastructure.

Also, OPS has conducted a vulnerability assessment that was used to identify which pipeline facilities are the "most critical." Because of their importance to meeting energy demands, and because of their proximity often to highly populated or environmentally sensitive areas, it is reasonable to assume that many pipeline systems were judged by OPS to be of a "critical" nature with respect to security considerations. DOT has not released the number of pipeline systems that they judged to meet this standard. OPS continues to work with various industry groups and state pipeline safety organizations "... to assess the industry's readiness to prepare for, withstand and respond to a terrorist attack on the nation's pipeline infrastructure."[17] OPS has warned that critical pipeline facilities, such as control centers, pump and compressor stations, as well as storage facilities may be targets for terrorist attacks. OPS assessments indicate that many of these facilities need to be better protected.[18]

OPS is working with several industry security task groups to assess vulnerabilities of pipeline facilities, identify specific actions that should be taken to strengthen protections at critical pipeline facilities, define different levels of criticality of pipeline facilities, and to develop plans to improve response and recovery preparedness.[19] Together with DOE and state pipeline agencies, OPS is promoting the development of consensus standards for security practices that OPS expects industry to implement at different levels of security threats at critical facilities. These different levels are now being tiered to correspond with the five levels of threat warnings that were issued by the Office of Homeland Security. [20] OPS is also developing a set of protocols for its personnel to use during inspections of pipeline facilities to ensure that operators are implementing appropriate security practices at critical facilities.

To convey emergency information and appropriate warnings, DOT has established a variety of communication systems with key staff at the "most critical" pipeline facilities throughout the country. OPS also has surveyed many pipeline companies to assess the security measures that have been taken since September 11. OPS is also identifying near-term technology to enhance deterrence, detection,

---

[16]Statement of Ellen Engleman. Subcommittee on Surface Transportation and Merchant Marine. Senate Committee on Commerce, Science, and Transportation. October 10, 2001.

[17]RSPA. OPS. RSPA Pipeline Security Preparedness. December 2001.

[18]U.S. DOT. RSPA. Budget Estimates Fiscal Year 2003. p. 106.

[19]Security measures may be tied to the level of criticality of a particular facility or segment of pipe.

[20]Statement of Ellen Engleman. Subcommittee on Energy and Air Quality. House Energy and Commerce Committee. March 19, 2002.

response and recovery, and is seeking to advance public and private sector planning for response and recovery.[21]

For many years, OPS has been conducting, with federal, state, and industry representatives, drills practicing emergency response to oil spills. The lessons learned from these exercises, as well as the formal and informal relationships established during these drills, could help prepare for releases caused by a terrorist attack of a pipeline systems. Emergency responders agree that it is much better to conduct planning and to develop relationships that improve coordination and response during a practice drill, than when there is an actual incident. Also, OPS is meeting with FERC, industry, and state agencies to explore recovery and response issues associated with possible terrorists attacks. Of concern is what strategies, authorities, and processes need to be in place, and what training and credentials need to be finalized in order to better plan for and respond to a terrorist attack.

It remains unclear when or which aspects of the security-oriented functions of OPS will be transferred to the new Transportation Security Administration within DOT. In view of this uncertainty, congressional oversight of the division of responsibility, possible transfer of personnel and funds, as well as legislative authorities may be warranted. Furthermore, as Congress debates reauthorization of pipeline safety legislation, it may be useful to consider the relative importance of OPS responsibilities regarding enhancement of safety, protection of the environment, and oversight of industry's security measures and capability to respond to terrorist incidents.

Illustrative Legislative Measures Pertaining to Pipeline Security[22]

The issue of pipeline security has been discussed primarily within the context of pipeline safety, energy policy and security legislation. One of the bills that includes specific provisions pertaining to pipeline security is H.R. 3609, the "Pipeline Infrastructure Protection To Enhance Security and Safety Act," which was introduced by Representative Don Young and others on December 28, 2001. Introduced on March 12, 2001 by Senator Jeff Bingaman and others, S. 517 (as amended), also popularly referred to as the "Energy Security Policy" bill, includes a provision pertaining to security-sensitive information on pipelines. Two other bills that include provisions pertaining to pipeline security are H.R. 3555, "United States Security (USA) Act of 2001," introduced by Representative Robert Menendez and others on December 20, 2001, and H.R. 3929, "Energy Pipeline Research, Development, and

---

[21]Statement of Ellen Engleman. Subcommittee on Highways and Transit. House Transportation and Infrastructure Committee. February 13, 2002.

[22]This report covers primarily bills pertaining specifically to pipeline operators, and mentions but does not emphasize illustrative legislation seeking to enhance the security of the Nation's critical energy infrastructure.

Demonstration Act," introduced by Representative Ralph Hall and others on March 12, 2002.[23]

H.R. 3609 specifies that the DOT Secretary is to require the operator of a pipeline facility to develop and implement a "terrorism security program," consisting of written procedures to follow and actions to take in the event of a terrorist attack on a pipeline facility or on other U.S. infrastructure facilities. The operator is to establish and implement reasonable procedures to safeguard the pipeline facility and safely maintain its operations. Those procedures are to include procedures for communicating with military, law enforcement, emergency service, and other appropriate governmental and non-governmental entities. The bill states that if DOT decides that a pipeline facility has a vulnerability to terrorist attacks, the Secretary may recommend that the operator of that facility take necessary actions to eliminate or reduce that vulnerability.

H.R. 3609 also requires the DOT Secretary to conduct a review of, and approve or disapprove, the security program of each pipeline operator. The bill also authorizes the Secretary to provide technical assistance to an operator of a pipeline facility, or to state, local, or tribal officials, to prevent or respond to acts of terrorism that may affect a pipeline facility. In addition, H.R. 3609 specifies that a person who knowingly and willfully damages or destroys, or attempts to damage or destroy, an interstate gas pipeline facility or interstate hazardous liquid pipeline facility, as an act of terrorism or for any other purpose, shall be fined under title 18, imprisoned for not more than 15 years, or both.

S. 517 (as amended) includes the previously passed Senate pipeline safety bill (S. 235) (with minor changes) plus a new provision pertaining to the protection of security-sensitive information regarding pipelines. The bill seeks to ensure that if DOT obtains such information, it is only released with adequate protection to specified parties. (H.R. 3609 includes a similar provision.) Many seek a balance between protecting information about the specific operating condition of a pipeline system that might be used by a terrorist to do harm and providing relevant information to citizen groups and others who are monitoring the performance and safety of a particular pipeline segment. Some are concerned that legislation to limit access to information about infrastructure vulnerability could allow companies to conceal data on safety challenges from those overseeing pipeline operations. On the other hand, others are concerned that easy access to security-sensitive information could endanger property and lives.

H.R. 3555 authorizes $5 million for fiscal year 2002 for the Secretary of Transportation to enter into an arrangement with the National Academy of Sciences for a comprehensive study of the security of energy pipelines, including issues related to monitoring, hardening of facilities, and hiring and training of security personnel. The bill also provides that not later than one year after the date of its enactment, the Secretary of Energy shall transmit to Congress a report describing the results of a risk management assessment of oil refineries and natural gas and liquid natural gas storage

---

[23]Hearings have been held on H.R. 3609 and discussions are underway that may lead to a markup of an amended bill. S. 517 passed the Senate as an amended version of H.R. 4. H.R. 3555 has been referred to several committees. H.R. 3929, as amended, was reported out of the House Science Committee.

facilities in the United States. The report is to include the results of a threat, vulnerability, and criticality assessment of such facilities. The bill authorizes $25 million for the study and $25 million for support of projects to demonstrate the best practices identified by the study and other appropriate topics.

H.R. 3929 authorizes $ 20 million for each of the fiscal years 2002 through 2006 for a cooperative federal program for research, development, demonstration, and standardization activities related to pipeline security, including improving the surveillance of pipeline rights–of–way, and for other purposes. The program would be conducted by the Department of Energy, DOT, and the National Institute of Standards and Technology in the Department of Commerce.

Concluding Observation

It is important to place the threat posed by terrorists to pipelines in perspective. Pipeline releases from corrosion, operator error, third-party damage, and other causes, are much more prevalent than intentional actions seeking to damage pipelines.[24] There are hundreds of unintentional releases from pipelines each year, and probably less than a handful, if that many, of intentional releases. Nevertheless, actions to reduce and planning to respond to the terrorist threat appears warranted because a well planned attack on a pipeline system located in a heavily populated area could result in a substantial number of deaths and injuries. Likewise, an attack on a system crossing or affecting an environmentally sensitive area could adversely affect water quality and wildlife. Because of the importance of pipeline security, continued congressional oversight to assess the adequacy and costs of OPS involvement in this area appears likely. Given the limited resources of the Pipeline Safety Fund, (which pays for most of the OPS program), several questions are raised:
If substantial funds and personnel resources are allocated towards security concerns, will implementation of OPS safety and environmental responsibilities be adversely affected? If some OPS resources are transferred to the TSA, how will this impact implementation of the more traditional OPS program?

[24] Statement of Lois N. Epstein. On behalf of Cook Inlet Keeper. Subcommittee on Highways and Transit Committee on Transportation and Infrastructure. February 13, 2002.