Order Code RL31990

Pipeline Security: An Overview of Federal Activities and Current Policy Issues

Updated February 5, 2004

Paul W. Parfomak
Specialist in Science and Technology
Resources, Science, and Industry Division

Pipeline Security: An Overview of Federal Activities and Current Policy Issues

Summary

Nearly half a million miles of oil and gas transmission pipeline crisscross the United States. The nation's pipeline industry has made substantial investments to protect these systems and respond to the possibility of terror attacks. However, U.S. pipelines are inherently vulnerable because of their number and dispersion. Due to the essential role pipelines play in our economy, Congress is examining the adequacy of federal pipeline security efforts.

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the lead federal agency for security in all modes of transportation — including pipelines. The agency oversees industry's identification and protection of critical pipeline assets through security reviews, risk assessment and inspections. The Office of Pipeline Safety (OPS), within the Department of Transportation (DOT), is the lead federal regulator of pipeline *safety*. While TSA and the OPS have distinct missions, pipeline security and safety are intertwined. There are questions about the appropriate division of responsibility between the agencies and about the resources they will have for mandated security activities.

As the lead agency for pipeline security, TSA expects pipeline operators to maintain security plans based on security guidance initially circulated in 2002. TSA also plans to issue pipeline security regulations, although it is unclear if and when it will do so. This agency also intends to issue new analytic models to help operators identify critical facilities and assess vulnerability to terrorist attack. In 2003, TSA inspected 24 of the largest 25-30 pipeline operators to review their security practices and collect critical asset data. TSA found that nearly all of these operators had met or exceeded minimum security guidelines. All but two of the 24 operators also provided TSA with their security plans and critical infrastructure information. The OPS joined TSA on approximately one-third of these inspections and expects a continued security role. The agencies have no formal cooperative agreement defining responsibilities and at this point do not think they need one.

Industry and government agencies generally assert that efforts to promote U.S. pipeline security are on the right track. Nonetheless, TSA's current funding for pipeline security will provide only limited capability for inspections and enforcement of any future regulations. The President' s FY2005 budget request does not include a line item for TSA's pipeline activities; they will be funded from the agency's general operational budget. In addition to appropriations issues, Congress is considering several policy concerns: Operators believe they need more specific federal threat information to improve security decisions. Many operators also believe they need clear and stable definitions of what constitutes a "critical" asset. Finally, operators are concerned about potentially redundant, conflicting regulatory regimes under TSA and the OPS. This report will be updated as events warrant.

Contents

List of Figures

Pipeline Security: An Overview of Recent Federal Activities and Current Policy Issues

Introduction

Nearly half a million miles of oil and gas transmission pipeline crisscross the United States.[1] These pipelines are integral to U.S. energy supply and have vital links to other critical infrastructure, like power plants, airports, and military bases. While an efficient and fundamentally safe means of transport, many pipelines carry volatile or flammable materials with the potential to cause public injury and environmental damage. The nation's pipeline networks are also widespread, running alternately through remote and densely populated regions; consequently, these systems are inherently vulnerable to terrorist attack. Pipeline operators have had security and emergency response programs in place for decades, but they have recently been taking steps to enhance those programs in response to new terrorist threats. Congress passed legislation to further encourage the pipeline industry to adopt better security practices, and to provide federal oversight of operator security programs (P.L. 107-71, P.L. 107-296, P.L. 107-355). Policy makers are now examining the progress and adequacy of these efforts.

This report provides an overview of recent federal activities related to pipeline security, including safety activities with links to security. The report describes the U.S. gas and oil pipeline networks, the industry's safety record and security risks, and the industry's security activities since September 11, 2001. It summarizes recent changes in federal pipeline security law and related changes in the security roles of federal agencies. The report discusses several policy concerns related to federal pipeline security efforts: 1) federal threat information for pipelines, 2) criteria for identifying "critical"assets, 3) TSA funding for pipeline security, and 4) federal agency cooperation in pipeline security.

Scope and Limitations

While this report addresses many safety issues related to security, it does not cover the full range of safety issues of potential interest to policy makers (e.g., inspection technology). Because the focus of this report is on activities and policies of federal agencies, it does not examine state pipeline agency activities in depth. The report also focuses on TSA and the OPS as the lead pipeline security and safety

---

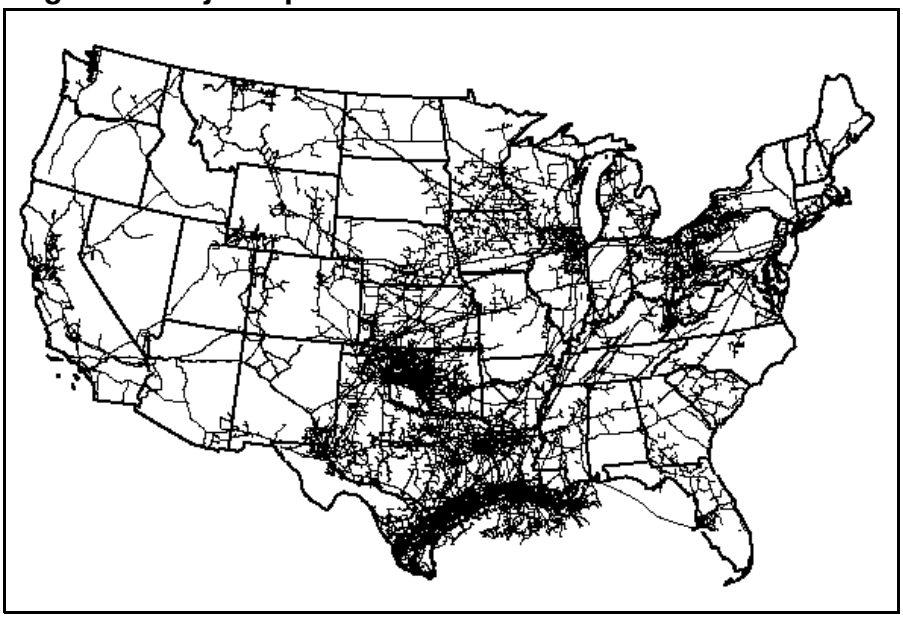
[1] Bureau of Transportation Statistics (BTS), *National Transportation Statistics 2002*, BTS02-08, December 2002, Table 1-10. In this report "oil" includes petroleum and other hazardous liquids such as gasoline, jet fuel, diesel fuel, and propane unless otherwise noted.

agencies. The activities of federal agencies with more limited roles in pipeline security and safety are reviewed in the Appendix.

Oil and Gas Pipeline Industry Overview

Some 470,000 miles of oil and gas transmission pipeline crisscross the United States, with links to Mexico and Canada. These pipelines run throughout the country, but the greatest concentration connects the major energy-producing regions in the South with the major energy-consuming regions in the Northeast (**Figure 1**).

Figure 1: Major Pipelines in the Continental United States



Source: Energy Information Administration

There are roughly 180,000 miles of oil pipeline in the United States carrying over 75% of the nation's crude oil and around 60% of its refined petroleum products.[2] Some 180 companies operate the *inter*state lines, which account for roughly 80 % of total pipeline mileage and transported volume.[3] The largest U.S. pipeline is the Trans Alaska Pipeline System (TAPS), which transports crude oil from Alaska's North Slope oil fields to the marine terminal in Valdez. TAPS runs some 800 miles and delivers roughly 17% of United States domestic oil production.[4] Like TAPS, major oil pipelines generally terminate at logistics hubs which typically link multiple pipelines, maintain substantial storage facilities and serve as gateways for regional distribution by truck, tanker, barge, or other means.

---

[2] BTS. December, 2002. Table 1-10.

[3] Trench, Cheryl J., *How Pipelines Make the Oil Market Work — Their Networks, Operation and Regulation.* Prepared for the Association of Oil Pipelines. Allegro Energy Group. New York, NY. December, 2001.

[4] Alyeska Pipeline Service Company. Internet home page. Anchorage, AK. 2003.

The U.S. natural gas pipeline network consists of around 210,000 miles of *inter*state transmission, plus approximately 75,000 miles of *intra*state transmission.[5] Around 80 systems make up the *inter*state network. Another 60 or so systems operate strictly within individual states.[6] These *inter*state and *intra*state transmission pipelines feed around 1.1 million miles of regional lines in some 1,300 local distribution networks.[7] Collectively, these gas pipelines transport nearly all of the natural gas in the United States. Gas pipelines serve electric generation and industrial customers directly, and link through "city gates" to regional distribution mains which, in turn, feed the local service lines of retail gas consumers. Some pipelines are also connected to liquefied natural gas (LNG) storage tanks which augment pipeline gas supplies during peak demand periods. According to the Department of Energy, there are 113 active LNG facilities in the U.S., mostly in the Northeast, many located near populated areas.[8]

Safety Record of the Pipeline Industry

Taken as a whole, releases from pipelines cause relatively few annual fatalities. Oil pipelines reported an average of 1.4 deaths per year from 1997-2001. Gas pipelines reported an average of 18.6 deaths per year during the same period.[9] It is difficult to make direct safety comparisons between pipelines and other transportation modes due to data limitations. Nonetheless, DOT statistics suggest that pipelines have much lower fatalities per ton-mile of general freight moved than truck, rail or waterborne transport. In general, the environmental safety record of oil pipelines is comparable to other transportation modes. According to the oil industry's own estimates, from 1995-2000 oil pipelines spilled an average of 0.9 gallons/million barrel-miles of oil, compared to 1.5 for trucks, 0.7 for rail and 0.7 for barges.[10] Similar direct comparisons for gas pipelines are not available.

Accidental pipeline releases result from a variety of causes, including outside force (e.g., third-party excavation), corrosion, mechanical failure, control system failure and operator error. Natural forces, such as floods and earthquakes, can also damage pipelines. According to the DOT, of 183 gas pipeline accidents reported in 2002, outside forces were by far the leading cause, accounting for 46% of reported failures. Outside forces was also the leading cause of the 140 oil pipeline accidents

---

[5] These figures exclude some 40,000 miles of field and gathering pipeline which connect gas extraction wells to collection and processing facilities.

[6] Tobin, James. *Natural Gas Transportation - Infrastructure Issues and Operational Trends*. Energy Information Administration (EIA). Washington, DC. October 2001.

[7] BTS. December, 2002. Tables 1-2 and 1-10.

[8] Energy Information Administration (EIA). *U.S. LNG Markets and Uses*. Washington, DC. January, 2003. p1.

[9] BTS. December, 2002. Tables 1-44 and 2-1. Natural gas ton-mile data are not reported.

[10] Trench, Cheryl J., *The U.S. Oil Pipeline Industry's Safety Performance*. Prepared for the Association of Oil Pipelines and the American Petroleum Institute. Allegro Energy Group. New York, NY. March, 2002. p29.

in 2002, responsible for 32% of failures.[11] These accident figures are significant in the context of security for two reasons: such releases happen much more frequently than is likely to occur from limited terrorist activity in the United States; and the pipeline industry has extensive experience responding to releases and generally does so relatively quickly.

Although pipeline releases have caused relatively few fatalities in absolute numbers, a single pipeline accident can be catastrophic. For example, a 1999 gasoline pipeline explosion in Bellingham, Washington killed two children and an 18-year-old man, and caused $45 million in damage to a city water plant and other property. In 2000, a natural gas pipeline explosion near Carlsbad, New Mexico killed 12 campers, including 4 children.[12] These accidents generated substantial scrutiny of pipeline regulation and increased state and community activism related to pipeline safety.[13] The accidents also highlighted the danger of pipelines as possible terror weapons because of their potential to harm people and damage property in their vicinity.

Pipeline Security Risks

Like any physical system, pipelines are vulnerable to vandalism and terrorist attack. The physical plant of these facilities may be damaged with explosives or by other mechanical means, disrupting flows and causing a release of pipeline contents. Alternatively, computer control systems may be "cyber-attacked," or both physical and cyber attack may happen at the same time. Some pipelines may also be indirectly disrupted by other types of terror strikes, such as attacks on regional electricity grids or telecommunications networks, which could in turn affect dependent pipeline control and safety systems.[14] Since pipelines supply fuel for vehicles, power plants, aircraft, heating, military bases and other uses, serious disruption of a pipeline network poses additional "downstream" risks.

Oil and gas pipelines have been a favored target of terrorists outside the United States. In Colombia, for example, rebels have bombed Occidental Petroleum's Caño Limón pipeline some 950 times since 1986, shutting it for months at a time and costing Colombia's government some $2.5 billion in lost revenues.[15] One of these

---

[11] Office of Pipeline Safety (OPS), US Department of Transportation (DOT). *Pipeline Incident Summary by Cause.* June 13, 2003. "Outside forces" includes damage from excavation, natural forces, vehicles and vandalism.

[12] National Transportation Safety Board (NTSB). *Pipeline Accident Report* PAR-03-01. Feb. 11, 2003.

[13] Nesmith, J. and Haurwitz, R.K.M. "Pipelines: The Invisible Danger." *Austin American-Statesman*. Austin, TX. July 22, 2001.

[14] Skolnik, Sam. "Local Sites Potential Targets for Cyberterror." *Seattle Post-Intelligencer*. Seattle, WA. Sept. 2, 2002.

[15] Marx, Gary. "Battle Over Colombian Pipeline Increasing U.S. Involvement in Civil War." *Knight Ridder Tribune News Service*. Washington, DC. Nov. 15, 2002.

attacks in 1998 caused a fire that killed or injured over 100 people.[16] In 1996, London police foiled a plot by the Irish Republican Army to bomb gas pipelines and other utilities across the city with 36 explosive devices.[17] In the last 2 years, oil and gas pipelines have also been attacked in Nigeria, Pakistan, Sudan, Myanmar and Iraq. In Saudi Arabia, a planned pipeline attack by al-Qaeda sympathizers at the country's main oil terminal was thwarted in 2002. Although it was unclear whether the planners had the capability to fully execute the Saudi attack, had they been successful, they could have disrupted the movement of over 6% of the world's daily oil consumption.[18]

Attacks and threats against pipelines and related infrastructure have also occurred in the United States. In 1997, Texas police prevented the bombing of natural gas storage tanks at a processing plant by Ku Klux Klan members seeking to create a diversion for a robbery (to finance other terrorist actions).[19] In 1999, Vancouver police arrested a man planning to blow up the trans-Alaska pipeline for personal profit in oil futures. He was found with high explosives and timers for 14 bombs.[20] In 2001, a vandal's attack with a high-powered rifle, also on the trans-Alaska pipeline, forced a two-day shutdown and caused extensive economic and ecological damage.[21]

Federal warnings about Al Qaeda threats since September 11, 2001 have repeatedly mentioned energy infrastructure broadly, and pipelines specifically, as potential terror targets in the United States.[22] These warnings included the discovery in late 2001 that computer hackers in the Middle East had infiltrated San Francisco area sites detailing information about local electricity systems, along with other critical infrastructure.[23] In June of 2003, U.S. intelligence agencies warned about a

---

[16] Anonymous. "Colombia Rebels Admit October Blast." *BBC Online Network*. London. October 20, 1998.

[17] President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures.* Washington, DC. October, 1997.

[18] Lumpkin, John J., "US Concerned al-Qaida Targeting Oil Interests in the Middle East", *Associated Press*. Washington, DC. October 16, 2002.

[19] Pressley, Sue Ann. "Group Planned Massacre and Big Robbery, FBI Says." *Washington Post*. Washington, DC. April 25, 1997. pA02.

[20] Cloud, David S., "A Former Green Beret's Plot to Make Millions Through Terrorism", *The Ottawa Citizen.* December 24, 1999. pE15.

[21] Rosen, Yereth. "Alaska Critics Take Potshots at Line Security." *Houston Chronicle*. February 17, 2002. p8.

[22] Anonymous. "Already Hard at Work on Security, Pipelines Told of Terrorist Threat." *Inside FERC*. McGraw-Hill Companies. Jan 03, 2002. See also: Federal Bureau of Investigation(FBI). *The Terrorist Threat Confronting the United States*. Statement of Dale L. Watson, Exec. Dir. for Counterterrorism and Counterintelligence before the Senate Select Committee on Intelligence. Washington, DC. February 6, 2002.

[23] Skolnik. 2002.

possible al-Qaeda attack on energy facilities, including pipelines, in Houston.[24] To date, there have been no actual attacks on these sites, but operators remain alert.

Despite substantial private and public efforts to promote security, it is widely recognized that pipelines are inherently vulnerable. The fact that pipelines run largely underground reduces their exposure to external threats, but required markings tell emergency responders, homeowners — and terrorists — where pipelines are located. Rather than trying to uniformly protect their entire systems, operators emphasize the security of especially vulnerable areas, such as river crossings, control centers, junctions, and storage tanks. They try to "harden" (i.e., to enhance the security of) these facilities and ensure adequate surveillance and monitoring. Operators also modify emergency plans to incorporate new elements of terror response, such as managing a federal crime scene.

Pipeline Safety and Security Regulation

The Natural Gas Pipeline Safety Act of 1968 (P.L. 90-481) and the Hazardous Liquid Pipeline Act of 1979 (P.L. 96-129) are two of the key early acts that specify the federal role in pipeline safety. Under both statutes, the Transportation Secretary is given primary authority to regulate key aspects of interstate pipeline safety: design, construction, operation and maintenance, and spill response planning. Pipeline safety regulations, some with security implications, are covered in Title 49 of the Code of Federal Regulations.[25] This title:

- Authorizes DOT to inspect pipelines and enforce its regulations with fines, injunctions, and criminal penalties
- Requires operators to report incidents, safety-related conditions and annual summary data
- Prescribes minimum pipeline safety requirements, including operator qualifications for regulated functions
- Imposes oil spill response plan requirements to reduce environmental impact of accidental discharges
- Provides grants-in-aid to state pipeline safety compliance agencies that adopt damage prevention programs
- Requires operators to establish drug and alcohol programs.

DOT administers pipeline regulations through the Office of Pipeline Safety (OPS) within the Research and Special Programs Administration (RSPA). The OPS has approximately 150 staff, including 100 inspectors generally located outside of Washington, D.C.[26] The OPS safety program is funded primarily by user fees assessed on a per-mile basis on each regulated pipeline operator (49USC60107).

---

[24] Hedges, Michael. "Terrorists Possibly Targeting Texas." *Houston Chronicle*. Houston. June 24, 2003.

[25] Safety and security of liquified natural gas (LNG) facilities used in gas pipeline transportation is regulated under CFR Title 49, Part 193.

[26] OPS. Personal communication. June 9, 2003.

Among other security-related provisions of P.L. 96-129 and subsequent laws, the OPS requires general protection of "exposed" oil pipeline facilities from vandalism and unauthorized entry.[27] The OPS also requires specified pipeline operators to establish written procedures for communicating with governmental response agencies and other public officials during emergencies.[28] Certain releases from oil or gas pipelines must be reported to DOT's National Response Center.[29] The OPS practices emergency response to oil spills with federal, state, and industry representatives. The lessons learned from these exercises, as well as the formal and informal relationships established during these drills, help prepare for releases in deliberate attacks.

Since 1997, the OPS has increasingly encouraged industry's implementation of "integrity management" programs on pipeline segments near "high consequence" areas. Integrity management provides for continual evaluation of pipeline condition; assessment of risks to the pipeline; inspection or testing; data analysis; and followup repair, as well as preventive or mitigative actions. High consequence areas include population centers, commercially navigable waters, and environmentally sensitive areas, such as drinking water supplies or ecological reserves. The integrity management approach directs priority resources to locations subject to the greatest consequences rather than applying uniform treatment to the entire pipeline network.[30] Integrity management risk assessments could be interpreted to include security, but the regulation does not explicitly address terrorism, and the OPS has provided "minimal" guidance to operators regarding terrorism risks expected in their plans.[31] The OPS made integrity management programs mandatory for most operators with 500 or more miles of regulated oil pipeline as of March 31, 2001 (49CFR195).

Pipeline Safety Improvement Act of 2002

On December 12, 2002, President Bush signed into law the Pipeline Safety Improvement Act of 2002 (P.L. 107-355). The act reauthorizes funding for the OPS through fiscal year 2006. It also strengthens federal pipeline safety programs, state oversight of pipeline operators, and public education regarding pipeline safety.[32]

---

[27] Code of Federal Regulations. 49 CFR 195.436.

[28] 49 CFR 192.605 and 192.615.

[29] 49 CFR195.52 and 191.

[30] Research and Special Programs Administration (RSPA).DOT. *Pipeline Safety. Pipeline Integrity Management in High Consequence Areas (Hazardous Liquid Operators with 500 or More Miles of Pipeline).* Fed. Register. Dec.1, 2000: 75378.

[31] OPS. Personal communication. June 9, 2003.

[32] P.L. 107-355 encourages the implementation of state "one-call" excavation notification programs (Sec. 2) and allows states to enforce "one-call" program requirements. The act expands criminal responsibility for pipeline damage to cases where damage was not caused "knowingly and willfully" (Sec. 3). The act adds provisions for ending federal-state pipeline oversight partnerships if states do not comply with federal requirements (Sec. 4).

Among other safety provisions, P.L. 107-355 requires operators of regulated gas pipelines in high consequence areas to conduct risk analysis and implement integrity management programs similar to those required for oil pipelines under 49CFR195. Integrity management, as a whole, is intended to focus primarily on safety, but certain elements may also have links to security, depending upon interpretation and application. For example, the integrity management rule for oil pipelines states that "identifying the need for additional preventive and mitigative measures, an operator must evaluate the likelihood of a pipeline release occurring and how a release could affect the high consequence area. This determination must consider all relevant risk factors..." (49CFR195.452). Guidance for this rule also cites "security of throughput (effects on customers if there is failure requiring shutdown)" as a risk factor for establishing assessment frequency.[33] As is the case for oil pipelines, the rule does not explicitly discuss risks from terror attacks. Nonetheless, assessment of accident risks near population centers could provide important data for related terror risk assessments. Likewise, system safety inspections could provide data useful for related security inspections.

P.L. 107-355 also:

- requires development of integrity management analysis and program standards by DOT within 12 months of enactment, and gas pipeline operator implementation within 24 months of enactment (Sec. 14),
- requires baseline integrity assessments of all high consequence area gas pipelines within 10 years, with reinspections every 7 years thereafter (Sec. 14),
- authorizes DOT to order safety actions for pipelines with potential safety problems (Sec. 7) and increases violation penalties (Sec. 8).

The criminal provisions under 49USC60123 amended by P.L. 107-355 state that

> "a person knowingly and willfully damaging or destroying, or attempting to damage or destroy, an interstate gas pipeline facility or interstate hazardous liquid pipeline facility shall be fined..., imprisoned for not more than 15 years, or both."

These provisions originally intended to deter unsafe excavators and vandals from damaging pipes could just as well apply to terrorists.

Pipeline operators have long been concerned about permitting and administrative barriers to emergency pipeline restoration efforts.[34] The act attempts to streamline this process by establishing an interagency committee, including the Department of Transportation, Environmental Protection Agency, Bureau of Land Management, Federal Energy Regulatory Commission, and other agencies, to ensure coordinated review and permitting of pipeline repairs (Sec. 16). In the event of a

---

[33] US Federal Register. Vol. 65. No. 232. December 1, 2000. p.75410.

[34] Haener, William J., CMS Energy Corp. Testimony on behalf of the Interstate Natural Gas Association of America (INGAA) before the House Transportation and Infrastructure Subcommittee on Highways and Transit. February 13, 2002. p6.

terror attack, expedited review and permitting could speed restoration by allowing operators to begin work quickly and to bypass damaged facilities by rebuilding through adjacent property or other alternate routes.

P.L. 107-355 authorizes $100 million for research and development in pipeline integrity, safety, and reliability (Sec. 12) including

> "the real-time surveillance of pipeline rights-of-way, developing tools for evaluating and enhancing pipeline security and infrastructure, reducing natural, technological, and terrorist threats, and protecting first response units and persons near an incident" (Sec. 12c5).

The act requires DOT to study ways to limit pipeline safety risks from population encroachment and ways to preserve environmental resources in pipeline rights-of-way (Sec. 11). P.L. 107-355 also includes provisions for public education, grants for community pipeline safety studies, "whistle blower" and other employee protection, employee qualification programs, mapping data submission and other provisions.

Integrity Management Support by the OPS

The provisions of P.L. 107-355 place significant new demands on the OPS. The act requires gas pipeline operators with facilities in "high consequence" areas to adopt new integrity management program plans by 2005, and to begin pipeline integrity assessments by mid-2006 (Sec 14.2). These gas pipeline plans will be in addition to oil pipeline integrity management plans required by 49CFR195. The act states that OPS "shall review a risk analysis and integrity management plan...and record the results of that review for use in the next review of an operator's program" (Sec 14.9A). According to the General Accounting Office (GAO), a comprehensive review of an integrity management plan by the OPS took about 2 weeks per plan in 2002.[35] Reviewing new integrity management plans in a timely manner, while sustaining its traditional pipeline safety oversight, will stretch the OPS' resources. GAO notes that "inspectors will face difficulties in judging the adequacy of complex integrity management processes that will vary from company to company."[36]

The OPS' enabling legislation allows the agency to delegate authority to *intra*state pipeline safety offices, and allows state offices to act as "agents"administering *inter*state pipeline safety programs (excluding enforcement) for those sections of *inter*state pipelines within their boundaries.[37] When effectively utilized, state inspectors are valuable resources for the OPS because they are familiar with local pipeline operations and can increase inspection thoroughness and frequency over what the OPS could do alone. In 2002, around 400 state pipeline safety inspectors (in 48 states, the District of Columbia and Puerto Rico) were

---

[35] General Accounting Office(GAO). *Pipeline Security and Safety: Improved Workforce Planning and Communication Needed.* GAO-02-785. August, 2002. p2.

[36] GAO. August, 2002. p13.

[37] United States Code. 49 USC 601. States may recover up to 50% of their costs for these programs from the federal government.

available.[38] The OPS plans to rely heavily on its state partners to inspect the integrity management programs of the *intra*state oil and gas pipelines. But the OPS must still administer a state's written assessments and related safety proposals (Sec 14.10). The agency faces additional challenges ensuring that state resources will be sufficient, training state inspectors in integrity management, and ensuring consistency among numerous state offices.[39]

The OPS intends to hire more federal inspectors to help meet the regulatory obligations of the integrity management rules. The President's FY2005 budget request for the OPS seeks $13 million for 168 full-time equivalent (FTE) employees, compared to an estimated $13 million for 156 FTE's in FY2004, and $10 million for 111 FTE's in FY2002. The budget also seeks $15 million in FY2005 for contract services, the same as in FY2004, but up from $5 million in FY2003.[40]

Pipeline Security Responses to September 11

Pipeline operators have always sought to secure their systems. While their security programs traditionally tended to focus on personnel safety and preventing vandalism, some have been more comprehensive. For example, security at the trans-Alaska pipeline during the Gulf War included measures such as armed guards, controlled access, intrusion detection and dedicated communications at key facilities, as well as aerial and ground surveillance of the pipeline corridor.[41] However, the events of September 11, 2001 focused attention on the vulnerability of pipelines to different terrorist threats. In particular, the terrorist attacks raised the possibility of systematic attacks on pipelines by sophisticated terror groups in a manner that had not been widely anticipated before.

After the September 11 attacks, natural gas pipeline operators immediately increased security and began identifying additional ways to deal with terrorist threats. Gas pipeline operators, for example, through the Interstate Natural Gas Association of America (INGAA), formed a security task force to coordinate and oversee the industry's security efforts. The INGAA states that it ensured that every member company designated a senior manager to be responsible for security. Working with DOT, the Department of Energy (DOE), and non-member pipeline operators, the INGAA states that it assessed industry security programs and began developing common risk-based practices for incident deterrence, preparation, detection and recovery. These assessments addressed issues such as spare parts exchange, critical parts inventory systems, and security communications with emergency agencies, among other matters. The INGAA also worked with federal agencies, including the

---

[38] GAO. *Pipeline Safety and Security: Improved Workforce Planning and Communication Needed.* GAO-02-785. Washington, DC. August 2002. pp5-6.

[39] GAO. August, 2002. p28.

[40] US Office of Management and Budget (OMB). *Budget of the United States Government, Fiscal Year 2005 — Appendix*. Washington, DC. February 2, 2004. p808.

[41] US General Accounting Office (GAO). *Trans-Alaska Pipeline: Ensuring the Pipeline's Security*. GAO/RCED-92-58BR. Washington, DC. November, 1991. p12.

OPS and Homeland Security, to develop a common government threat notification system.[42]

The natural gas companies reported significant commitments to bolster security at their critical facilities. According to the American Gas Association (AGA), companies strengthened emergency, contingency and business continuity plans; increased liaison with law enforcement; increased monitoring of visitors and vehicles on pipeline property; monitored pipeline flows and pressure on a continuous basis; increased employee awareness to security concerns; and deployed additional security personnel.[43] The industry also began developing encryption protocol standards to protect gas systems from cyber attack.[44] Operators also sought redundancy in the delivery system to provide greater flexibility to redirect or shut down product flows.

The oil pipeline industry responded to the September 11 attacks in a manner similar to that of the gas pipeline industry. Pipeline operators reviewed procedures, tightened security, rerouted transportation patterns, closely monitored visitors and made capital improvements to harden key facilities.[45] Operators also increased surveillance of pipelines, conducted more thorough employee background checks, and further restricted Internet mapping systems.[46] The Association of Oil Pipe Lines (AOPL) and the American Petroleum Institute (API), working together, provided guidance to member companies on how to develop a recommended pipeline security protocol analogous to an existing protocol on managing pipeline integrity. Along with the gas pipeline industry, the oil pipeline industry reconciled its levels of security threat and associated measures with the national threat advisory system of the Office of Homeland Security. According to the AOPL, 95 percent of oil pipeline operators had developed new security plans and had instituted the appropriate security procedures by February, 2003. The remaining 5 percent are primarily small operators in other businesses but with oil pipelines between plant facilities.[47]

In conjunction with the Office of Homeland Security, pipeline operators joined with other gas and oil companies to establish an Information Sharing and Analysis Center (ISAC) in November 2001. The ISAC is a cooperative, industry-directed database and software applications center for information related to security, including real-time threat alerts, cyber alerts and solutions. The ISAC allows authorized individuals to submit reports about information and physical security

---

[42] Haener, William J. February 13, 2002. p4.

[43] American Gas Association (AGA) *Natural Gas Distribution Industry Critical Infrastructure Security*. 2002. and AGA. *Natural Gas Infrastructure Security — Frequently Asked Questions.* April 30, 2003.

[44] Ryan, Karen. "Powerful Protection." *American Gas*. Washington, DC. May, 2002.

[45] Shea, William H., President and CEO, Buckeye Pipe Line Co. Testimony on behalf of the Association of Oil Pipe Lines (AOPL) and the American Petroleum Institute (API) before the House Transportation and Infrastructure Subcommittee on Highways and Transit. February 13, 2002.

[46] Association of Oil Pipelines (AOPL). "Protecting Pipelines from Terrorist Attack." *In the Pipe*. Washington, DC. February 10, 2003.

[47] AOPL. February 10, 2003.

threats, vulnerabilities, incidents, and mitigation. The ISAC also provides access to information from other members, U.S. government and law enforcement agencies, technology providers, and other security associations.[48] In 2003, the ISAC had limited participation by operators since members were required to pay fees and similar information was available directly from other sources. The energy industry has taken steps, such as hiring a new administration contractor, to increase the usefulness of the ISAC and increase its membership.[49]

Response of the Office of Pipeline Safety

Presidential Decision Directive 63 (PDD-63) issued during the Clinton administration assigned lead responsibility for pipeline infrastructure protection to the DOT.[50] At the time, these responsibilities fell to the OPS, since the agency was already addressing some elements of pipeline security in its role as safety regulator. Immediately after September 11, 2001, the OPS issued several emergency bulletins to oil and gas pipeline companies communicating the need for a heightened state of alert in the 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."[51]

Soon thereafter, because of national security concerns, the OPS removed from its web site detailed maps of the country's pipeline infrastructure.

The OPS also conducted a vulnerability assessment used to identify which pipeline facilities were "most critical" because of their importance to meeting national energy demands or proximity to highly populated or environmentally sensitive areas. The OPS worked with industry groups and state pipeline safety organizations "... to assess the industry's readiness to prepare for, withstand and respond to a terrorist attack..."[52] The OPS warned that critical pipeline facilities, such as control centers, pump and compressor stations, and storage facilities, might be targets — and that many of these facilities needed to be better protected.[53]

---

[48] Energy Information Sharing and Analysis Center. *About the Energy ISAC*. Internet home page. Washington, DC. May 2003.

[49] American Gas Association (AGA). Personal communication. June 11, 2003.

[50] Presidential Decision Directive 63. *Protecting the Nation's Critical Infrastructures*. May 22, 1998.

[51] Engleman, Ellen. RSPA, Administrator. Statement before the Subcommittee on Surface Transportation and Merchant Marine. Senate Committee on Commerce, Science, and Transportation. October 10, 2001.

[52] RSPA. *RSPA Pipeline Security Preparedness*. December, 2001.

[53] RSPA. Budget Estimates Fiscal Year 2003. p106.

Through 2002, The OPS was the federal agency most active in encouraging industry activities intended to better secure the nation's pipelines. In general, The OPS' approach was to encourage operators to voluntarily improve their security practices rather than to develop new security regulations. In adopting this approach, The OPS sought to speed adoption of security measures by industry and avoid the publication of sensitive security information (e.g., critical facility lists) that would normally be required in public rulemaking.[54]

The OPS worked with several industry security task groups to define different levels of "criticality," to identify actions to strengthen protection based on this criticality, and to develop plans for improved response preparedness. The OPS surveyed many pipeline companies to assess security measures taken since 9/11. Together with DOE and state pipeline agencies, the OPS promoted the development of consensus standards for security measures tiered to correspond with the five levels of threat warnings issued by the Office of Homeland Security.[55] The OPS also developed protocols for inspections of critical facilities to ensure that operators implemented appropriate security practices. To convey emergency information and warnings, the OPS established a variety of communication links to key staff at the most critical pipeline facilities throughout the country. The OPS also began identifying near-term technology to enhance deterrence, detection, response and recovery, and began seeking to advance public and private sector planning for response and recovery.[56]

On September 5, 2002, The OPS circulated formal guidance defining the agency's security program recommendations and implementation expectations. This guidance recommended that operators identify critical facilities, develop security plans consistent with prior trade association security guidance, implement security plans and review those plans annually.[57] The guidance defined asset "criticality" in terms of threats, risks to people, and economic impacts from the loss of energy supply. It also suggested specific security measures to be taken at the 5 different homeland security threat levels, with over 50 cumulative measures at the highest threat level. While the guidance was voluntary, the OPS expected compliance from operators of critical facilities. The agency believed it had the authority to enforce the requirements if voluntary compliance was not effective. The OPS asked operators for a written statement certifying their compliance within 6 months. The OPS also informed operators of its intent to begin reviewing security programs within 6

---

[54] GAO. *Pipeline Security and Safety: Improved Workforce Planning and Communication Needed.* GAO-02-785. August, 2002. p22.

[55] Engleman, Ellen. RSPA, Administrator. Statement before the Subcommittee on Energy and Air Quality. House Energy and Commerce Committee. March 19, 2002.

[56] Engleman, Ellen. RSPA, Administrator. Statement before the Subcommittee on Highways and Transit. House Transportation and Infrastructure Committee. February 13, 2002.

[57] O'Steen, James K., RSPA, Deputy Associate Administrator For Pipeline Safety. *Implementation of RSPA Security Guidance*. Presentation to the National Association of Regulatory Utility Commissioners. February 25, 2003.

months of the certification deadline, potentially as part of more comprehensive safety inspections.[58]

Transportation Security Administration

In November, 2001, President Bush signed the Aviation and Transportation Security Act (P.L. 107-71) establishing the Transportation Security Administration (TSA) within DOT. The act accorded TSA with responsibility for security "in all modes of transportation, including "...modes of transportation that are exercised by the Department of Transportation." According to TSA, this provision placed DOT's pipeline security authority (under Presidential Decision Directive 63) within TSA. The act specified for TSA a range of duties and powers related to general transportation security, such as intelligence management, threat assessment, mitigation, security measure oversight and enforcement, among others. Due to high public concern about aviation, however, and aviation-related deadlines specified in the act, TSA focused primarily on aviation security during its first year of existence.[59]

On November 25, 2002, President Bush signed the Homeland Security Act of 2002 (P.L. 107-296) creating the Department of Homeland Security (DHS). Among other provisions, the act transferred to DHS the Transportation Security Administration from DOT (Sec. 403). During 2003, TSA increased its focus on transportation modes beyond aviation. According to TSA officials, the agency took the lead as the national transportation security manager for pipeline security, building upon prior federal efforts and relationships (particularly those with the OPS) to do what it could "to protect the critical infrastructure from terrorists."[60] These efforts were led by the Pipelines Branch in TSA's Transportation Infrastructure Security division.

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) clarifying executive agency responsibilities for identifying, prioritizing and protecting critical infrastructure. HSPD-7 maintains DHS as the lead agency for pipeline security (Par. 15), and instructs DOT to "collaborate in regulating the transportation of hazardous materials by all modes (including pipelines)" (Par. 22h). The order also requires that DHS and other federal agencies collaborate with "appropriate private sector entities" in sharing information and protecting critical infrastructure (Par. 25). HSPD-7 supersedes PDD-63 (Par. 37).

TSA Pipelines Branch Activities

TSA's Pipeline Branch is implementing its plans with respect to pipeline security inspections, standards development, and critical asset analysis. According to TSA, the agency expects pipeline operators to maintain security plans based on the OPS/industry consensus security guidance circulated in 2002 and subsequent

---

[58] RSPA. Personal communication. June 10, 2003.

[59] TSA. Personal communication. May 28, 2003.

[60] Fox, Jack. TSA, Branch Chief, Pipelines. Remarks to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

revisions.[61] In 2003 the agency visited 24 of the largest 25-30 pipeline operators to review their security plans and inspect their facilities. The agency plans to complete the remaining large operator inspections by April 2004, and then begin inspections of major gas distribution systems. During the reviews, TSA evaluates whether each company has followed the intent of the OPS/industry security guidance, and seeks to collect the list of assets each company has identified meeting the criteria established for critical facilities. According to TSA, nearly all operators visited by the agency have met the minimum security guidelines, and some have gone "way beyond" the minimum requirements. All but two of the 24 operators have provided TSA with copies of their security plans and system maps, as well as critical infrastructure information. The two operators declining to provide this information did not believe they had adequate assurances the information would be protected from public disclosure. The OPS joined TSA on approximately one-third of its operator inspections in 2003.[62] TSA seeks the OPS' participation in these reviews, but does not require it.[63]

TSA's FY2005 budget justification maintains that the agency "will... issue regulations where appropriate to improve the security of the [non-aviation transportation] modes."[64] Accordingly, TSA ultimately intends to establish pipeline security regulations to move beyond voluntary compliance, as is now the case, and provide a clear basis for future enforcement. The agency believes such regulations may be necessary because it believes existing OPS safety regulations provide only limited enforcement authority in security, especially counter-terrorism. TSA has begun the process of developing new pipeline security regulations, but it is not clear when TSA will actually issue them. TSA believes it has the OPS' agreement that future TSA security plans will be the only ones required of operators and that TSA will be responsible for reviewing them.[65]

According to TSA, the agency intends to work with industry to help operators better identify their most critical assets. Industry has been assessing asset criticality under the current security guidance, but TSA plans to publish a new multi-modal (including pipelines) model providing a clearer basis for identifying assets that might be subject to terrorist attacks. The model accounts for potential loss of human life and well-being (e.g., illness, access to emergency services), reconstitution, economic impact, and symbolic importance. TSA expects assessments to be conducted initially within each transportation mode, with final assessments across all transportation modes. TSA intends to use the model results for allocating resources to protect the highest priority assets across different modes of transportation. TSA's

---

[61] TSA. Personal communication. January 12, 2004.

[62] TSA. Personal communication. January 12, 2004.

[63] TSA. Personal communication. May 22, 2003.

[64] Department of Homeland Security (DHS). Transportation Security Administration Fiscal Year 2005 Congressional Budget Justification. Washington, DC. p20. Feb. 2, 2004.

[65] TSA. Personal communication. February 4, 2004.

Pipeline Branch has been developing, and plans to maintain in the future, its own inventory of critical pipeline infrastructure based on this model.[66]

The TSA has also been developing a new multi-modal asset vulnerability tool, the Transportation Risk Assessment and Vulnerability Evaluation (TRAVEL) model, which it expects the major transportation modes (including pipelines) to use for evaluating the vulnerability of critical assets. According to TSA staff, the model should evaluate operator security plans based on a set of pre-determined relevant and realistic "attack scenarios." For pipelines, these scenarios specify a variety of physical and cyber-attacks to the network, including attacks incorporating chemical and biological agents. By applying one model across transportation modes, TSA seeks to establish a more consistent approach to assessing vulnerability than mode-specific models might provide.[67] According to TSA, the TRAVEL model has not yet been finalized and expanded to include pipelines, although it has already been used in other transportation modes.[68]

In addition to the activities above, TSA intends to establish qualifications for personnel seeking unrestricted access to critical transportation assets, including pipeline assets. TSA has also been addressing legal issues regarding recovery from terrorist attacks, such as FBI control of crime scenes and eminent domain or property seizure in pipeline restoration around a crime scene.[69]

Key Policy Issues in Pipeline Security

Government and industry have taken substantial actions during the last two years to improve pipeline security and oversight. As one industry executive remarked, "Before 9/11, we never contemplated somebody flying a jet into some critical facility we have. Now we not only think about it, but we're also putting very different contingency plans in place."[70] Federal agencies acknowledge industry's progress. The President's 2003 infrastructure protection strategy, for example, noted that "pipeline facilities already incorporate a variety of stringent safety precautions" and that "as a whole, the response and recovery capabilities of the pipeline industry are well proven..."[71] Senior DHS officials have also asserted that "pipelines are the

---

[66] TSA. *TSA Multi-Modal Criticality Evaluation Tool.* TSA Threat Assessment and Risk Management Program. Slide presentation. April 15, 2003.

[67] TSA. Personal communication. May 28, 2003.

[68] TSA. Personal communication. Feb. 4, 2003

[69] TSA. Personal communication. May 28, 2003.

[70] Donald Field, ExecutiveV.P., People's Energy Corp., Chicago, IL. as quoted in Ryan, Karen. "Powerful Protection." *American Gas*. Washington, DC. May, 2002.

[71] Office of the President. *The Physical Protection of Critical Infrastructure and Key Assets.* February, 2003. p 58.

best organized and have the best security practices" among maritime and land transportation sectors.[72]

Notwithstanding the progress to date in improving pipeline security, continued implementation of industry and government programs faces several challenges. As discussed in detail in the following sections, many in industry are concerned about the quality of information about actual terrorism threats that they receive from DHS. Industry is also generally concerned that criteria for identifying critical facilities continue to evolve. As a result, the pipeline industry is concerned that it may be forced to spend too much on pipeline security, or spend in the wrong places — diverting limited resources from safety programs and other important uses. TSA faces resource constraints of its own, limiting the agency's ability to improve industry security standards and oversee pipeline security in the field. TSA and the OPS currently cooperate on security inspections, but many in industry are still concerned about the possibility of redundant, conflicting regulatory regimes.

Federal Threat Information

The DHS' Homeland Security Advisory System communicates terrorist threats to the public based on five threat conditions: low, guarded, elevated, high and severe (represented by the colors green, blue, yellow, orange and red).[73] The pipeline industry's security guidance links specific security measures to these five threat levels. While this approach ensures some consistency in terror preparedness among pipeline systems, many operators believe they require more specific threat information to make better security decisions and focus protection where it is truly needed. For example, these operators question whether an "orange" DHS threat level applies equally across the country.[74] By uniformly responding to what they perceive as ambiguous warnings, operators believe they may expend scarce resources to bolster security at facilities that are not really under increased threat. Furthermore, operators do not believe federal agencies have been as effective as they could be communicating the specific threat information they do receive. According to one industry representative, "CNN tells us first, then we hear from FBI, DOE and other agencies."[75]

Concerns about non-specific threat information are not endemic to pipelines, however, and they are not new. DHS Secretary Ridge has acknowledged that the current color-coded terror alert system needs improvement to provide greater "granularity." He expressed the department's intention to create a system that could raise threats for specific industries or geographic areas without changing threat levels

---

[72] Liscouski, Robert. DHS, Asst. Secy. for Infrastructure Protection. Remarks to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

[73] DHS. *Homeland Security Advisory System.* Washington, DC. June 13, 2003.

[74] AGA. Personal communication. June 11, 2003.

[75] AGA. Personal communication. June 11, 2003.

elsewhere. However, Secretary Ridge also commented that information on terrorist movements was still too vague for such specific warnings.[76]

Identifying Critical Facilities

Various industry representatives state that they need clear and stable definitions of pipeline asset criticality so they will know exactly what assets to protect, and how well to protect them. Otherwise, the pipeline industry risks hardening too many facilities, hardening the wrong facilities, or both. Either outcome would increase ultimate costs to consumers without commensurate security benefits, and could potentially divert scarce security resources from better uses within or outside the pipeline industry (e.g., securing electric power stations).

Despite the security guidance put forward by the OPS in 2002, pipeline operators are still uncertain how regulators will ultimately identify critical facilities — and what protections regulators will expect for them. The definition of criticality developed by industry in 2002 (and supported in the OPS' guidance) avoided numerical thresholds, relying instead on discretionary qualitative metrics like "significance" of impact.[77] The OPS has expressed its belief that this criticality definition may be too general and that clearer criticality thresholds are needed.[78] The HSPD-7 directive appears to narrow the definition of "criticality" by emphasizing "infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties" (Par. 13). It is not clear, however, how this emphasis will change what is considered to be critical pipeline infrastructure.

The pipeline industry is also concerned that, in its efforts to ensure consistency among transportation modes, TSA will not appropriately treat pipeline assets as unique (non-vehicular) transportation and a key component in the nation's broader energy infrastructure.[79] For example, many are concerned that threshold parameters such as "fair market value of lost asset" in TSA's model might not appropriately account for the downstream economic impact of disrupted gas or oil supplies.[80]

Pipeline Security Resources at TSA

The President's FY2005 budget request for DHS does not include a separate line item for TSA's pipeline security activities. The budget request does include a $146 million line item for "Transportation Security Enterprise," which encompasses all

---

[76] Shenon, Philip. "Threats and Responses: Domestic Security." *The New York Times*. New York. June 5, 2003. pA15.

[77] American Gas Association (AGA) and the Interstate Natural Gas Association of America (INGAA). *Security Guidelines Natural Gas Industry Transmission and Distribution*. Washington, DC. September 6, 2002. p6.

[78] OPS. Personal communication. June 9, 2003.

[79] Cooper, Benjamin S. AOPL, Executive Director. *Pipeline Security Planning*. Presentation to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

[80] AOPL. Personal communication. June 5, 2001.

security activities in non-aviation transportation modes, including pipelines.[81] According to TSA's budget office, the Pipelines Branch receives from the agency's general operational budget "a normal allocation for routine operations" such as regulation development, travel, and outreach.[82] According to TSA's pipeline branch, the current budget will fund five full-time staff, the same staff level as in FY2004. These staff will maintain TSA's asset database, support TSA's multi-modal risk models, develop new security standards and issue regulations — all with the consultation of industry and other federal agencies. In addition, TSA staff will conduct pipeline security inspections and enforce any future security regulations.[83]

At its current staffing level, TSA's Pipelines Branch has limited field presence for inspections and possible enforcement of future regulations, an issue of particular concern to TSA.[84] (For comparison, the OPS can deploy around 500 federal and state safety inspectors across the same pipeline network.) According to TSA, the agency cannot now use OPS inspectors extensively for security work because the OPS faces resource constraints of its own; only a handful of OPS inspectors are trained in security; and even if the OPS could "lend" inspectors to TSA, the agency would require compensation TSA cannot currently offer.[85] Furthermore, it is not clear that TSA has a mechanism under law to delegate inspection authority to state agencies like the OPS does. Even if TSA did have such a mechanism, states appear generally unwilling to take on this responsibility, lack the required security inspection skills, and might not be able to adequately safeguard security information.[86] The TSA is reluctant to use contractors for field work because the pipeline industry is concerned about safeguarding security information.[87]

TSA's plan to focus security inspections, at least initially, on the largest pipeline and distribution system operators seeks to make the best use of limited staff. It is an open question, however, how many of the remaining operators — some 1,000 systems — should also be inspected. Criticality assessment and risk analysis are still evolving, so the basis for prioritizing one set of pipelines over another for security purposes is debatable. For example, while possibly less critical from a national perspective, smaller pipeline systems still present local security risks, and could arguably be more vulnerable than larger systems if they have smaller security budgets and fewer staff dedicated to infrastructure protection. Without security plan verification and a credible threat of enforcement, operator compliance with security guidance may be inadequate, leaving the pipeline network as a whole less secure than it might be with more universal inspection and enforcement coverage.

---

[81] US Office of Management and Budget (OMB). *Budget of the United States Government, Fiscal Year 2005 — Appendix*. Washington, DC. February 2, 2004. p485.

[82] TSA. Personal communication. June 11, 2003.

[83] TSA. Personal communication. Feb. 4, 2004.

[84] TSA. Personal communication. May 28, 2003.

[85] TSA. Personal communication. May 28, 2003.

[86] RSPA. Personal communication. June 10, 2003.

[87] TSA. Personal communication. June 19, 2003.

OPS and TSA Cooperation on Pipeline Security

The relationship between the OPS and TSA on pipeline security matters is still evolving, but appears to be generally cooperative. While TSA believes it has an understanding with the OPS that TSA will be the lead agency for pipeline security, a memorandum of agreement between the agencies has not been signed. According to agency correspondence, when DHS was created, Transportation Secretary Mineta did not believe that a formal agreement between TSA and the OPS would be necessary because the two agencies were already working together.[88]

The OPS sees a strong link between pipeline security and safety. One senior agency administrator has asserted that "safety and security are interdependent...the distinction is a function of intent to do damage."[89] In the context of its ongoing safety activities, the OPS maintains that "pipeline integrity is a broad umbrella covering safety, security and reliability."[90] Nonetheless, the OPS acknowledges TSA's superior access to information on threats and vulnerabilities, as well as TSA's broader multi-sector perspective. Accordingly, OPS staff believe that while the OPS will not be the major player in pipeline security, the agency will always have a role. In particular, according to the OPS, the agency plans to ensure that pipeline security measures do not adversely impact pipeline safety.[91] In the short term, the OPS plans to independently conduct security spill and response exercises and, with TSA, to jointly inspect operator security plans based on its security guidance of last year.[92] The OPS has not, however, made a long-term commitment to security inspections, currently using only minimal resources in the form of a few staff working part-time with TSA.

The pipeline industry is generally concerned that it might face redundant, conflicting regulatory regimes under different agencies with "teams from government stumbling over each other to inspect pipes."[93] Consequently, TSA believes a sharper distinction ultimately may be needed between its security activities, and the safety activities of the OPS. TSA is concerned that too much OPS involvement in pipeline security may create confusion among operators as to which agency is in charge of security and what requirements may be in force. The OPS and TSA believe their responsibilities have been worked out, however, without the need for formal agreements. The agencies are engaged in ongoing roundtable discussions with the

---

[88] Mineta, Norman Y., Secretary of Transportation. Letter to James M. Loy, Under Secretary for Transportation Security, Department of Transportation. February 27, 2003.

[89] Bonasso, Samuel. RSPA, Acting Administrator, Remarks to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

[90] O'Steen, James. RSPA, Deputy Assoc. Admin., Pipeline Safety. Remarks to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

[91] RSPA. Personal communication. June 10, 2003.

[92] O'Steen, James. May 22, 2003.

[93] Badolato, Edward. Shaw Group. Remarks to the International Pipeline Safety/Security Conference. E.J. Krause Associates. Arlington, VA. May 22, 2003.

pipeline trade associations and FERC to address additional concerns as they emerge.[94]

The Pipeline Security Challenge in Perspective

U.S. pipeline operators currently report no specific threats to their networks — but the nation's's pipeline system is extensive and presents an inviting target. It is widely accepted that protecting their assets better is in the best interest of operators, and federal agencies are monitoring and encouraging these efforts. As a practical matter, industry and government could spend vast sums to enhance pipeline security — but this investment would have to be balanced against many other investment needs and opportunities. The OPS and TSA face resource limitations and have many other priorities besides pipeline security concerns. Furthermore, it is widely held that pipelines are already safer and more secure than most other critical infrastructures. While the pipeline industry continues to face challenges protecting its assets, many analysts believe that more urgent security challenges lie elsewhere.

Conclusions

Both government and industry have taken numerous steps to try to improve pipeline security. Federal activities in this area are relatively new and agency responsibilities are still being sorted out, but discussions with a variety of industry representatives suggest that these efforts are generally thought to be moving in a logical direction. Furthermore, ongoing dialogue among the operators and federal agencies appears to be addressing many elements of federal pipeline security policy that have been causing concern.

As oversight of the federal role in pipeline security continues, questions may be raised concerning the existing resources of TSA and its ability to execute its various pipeline security responsibilities, especially the implementation and enforcement of any potential future pipeline security regulations. Congressional policymakers may pose questions: Are TSA's pipeline security activities adequately funded? Is there a solid basis for how TSA prioritizes the most "critical" pipeline systems so that important network security vulnerabilities are not overlooked? Should TSA inspect more pipeline systems to ensure universal compliance with security guidelines? Is there an appropriate division of responsibility for pipeline security among the federal agencies to minimize the possibility of regulatory confusion and best balance agency missions with capabilities?

In addition to these specific issues, Congress may wish to assess how the various elements of U.S. pipeline security activity fit together in the nation's overall strategy to protect critical infrastructure. For example, increasing the number of pipeline security inspections by TSA could be of limited value if asset "criticality" is not clearly defined and federal threat information remains ambiguous. Likewise, diverting pipeline resources away from safety to enhance security might further reduce terror risk, but not overall pipeline risk, if safety programs become less

---

[94] AGA. Personal communication. June 11, 2003.

effective as a result. U.S. pipeline security necessarily involves many groups: federal agencies, oil and gas pipeline associations, large and small pipeline operators, and critical and non-critical asset owners. Reviewing how these groups work together to achieve common security goals could be an oversight challenge for Congress.

Appendix: Pipeline Security Activities of Other Federal Agencies

Federal Infrastructure Security Agencies

The Critical Infrastructure Assurance Office (CIAO), created by PDD-63 as an interagency office within the Commerce Department in 1998, was charged with coordinating federal critical infrastructure assurance initiatives and raising industry awareness of infrastructure risks, especially those related to information systems.[95] Among other activities, CIAO facilitated private sector (including oil and gas) input to the national strategy for critical infrastructure through the Partnership for Critical Infrastructure Security, and helped support formation of the Energy Information Sharing and Analysis Center (ISAC).[96]

The National Infrastructure Protection Center (NIPC) within the FBI was also created by PDD-63 in 1998. The mission of the NIPC was to detect, prevent, respond to and investigate malicious acts against the nation's critical infrastructures. NIPC was a primary source of threat information to the Energy ISAC, and also worked with industry on national critical infrastructure strategy. The NIPC was viewed by industry as "a central focus for law enforcement and incident analysis, but not the central point for all forms of private sector cooperation."[97]

The Office of Energy Assurance (OEA) was established within the Department of Energy by Secretary Abraham in May, 2001 to help protect the country against major energy supply disruptions. While the DOE is not responsible for pipeline security, its activities under PDD-63 as the lead agency for all other energy security has had implications for oil and gas pipelines. For example, OEA co-sponsored the development of guidelines for municipal governments to respond to natural gas supply disruptions.[98] The OEA's National Infrastructure Simulation and Analysis Center (NISAC) was chartered under Section 1016 of the USA Patriot Act (P.L. 107-56) in October, 2001. The NISACs's stated mission has been to provide new computer modeling and simulation capabilities for critical infrastructure analysis focusing on interdependencies, vulnerabilities, and complexities.[99] NISAC has

---

[95] PDD-63. May 22, 1998.

[96] Watson, Kenneth C., President, Partnership for Critical Infrastructure Security. Testimony before the House Energy and Commerce Committee, Subcommittee on Oversight and Investigation. July 9, 2002.

[97] Montgomery, Mark. "Cybersecurity Policy: Moving from Nouns to Verbs." *Security in the Information Age: New Challenges, New Strategies*. U. S. Congress Joint Economic Committee. May, 2002. p29.

[98] Office of Energy Assurance (OEA.). *Planning for Natural Gas Disruptions: Critical Infrastructure Assurance Guidelines for Municipal Governments (Review Draft)*. Chicago Metropolitan Area Critical Infrastructure Protection Program. August, 2002 .

[99] National Infrastructure Simulation and Analysis Center (NISAC). Sandia National (continued...)

promoted, among other capabilities, the ability to assess the propagation and escalation of minor initiating events between energy, communication and water infrastructures.[100]

The Homeland Security Act of 2002 transferred the activities of the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, and the Office of Energy Assurance (Sec. 201) into the new Information Analysis and Infrastructure Protection (IAIP) Directorate of DHS. The stated mission of IAIP is to "analyze intelligence and information from other agencies (including the CIA, FBI, DIA and NSA) involving threats to homeland security and evaluate vulnerabilities in the nation's infrastructure."[101] Among other activities, IAIP intends to evaluate cross-infrastructure (e.g., energy, transportation and telecom) dependencies from the broadest perspective, building on criticality and vulnerability analysis done by the separate infrastructure sector lead agencies — such as TSA for pipelines. IAIP also intends to offer guidance on "protection action strategies" with the overall goal of "enabling protection with better information." IAIP also intends to dedicate "technical experts" to facilitate analysis done by the infrastructure sector leaders and their industry partners, but will not seek direct regulatory relationships with industry unless sector lead agencies fail to do so.[102]

Department of Justice

In addition to greater oversight of pipelines by regulatory agencies, the Department of Justice (DOJ) has increased its enforcement activities related to pipelines. For example, on January 22, 2003, the Justice Department, with the Environmental Protection Agency and the state of Washington, announced a settlement with Olympic Pipeline Co. and Shell Pipeline Co., resolving claims from the Bellingham pipeline accident. That settlement imposed some $92 million in civil fines and enhanced spill prevention spending, on top of $21 million in penalties imposed in related criminal proceedings.[103]

On March 11, 2003, emphasizing the environmental aspects of homeland security, Attorney General Ashcroft announced a crack down on companies failing to protect against possible terrorist attacks on storage tanks, transportation networks, industrial plants — and pipelines. He pledged to increase prosecution of civil and criminal cases, where appropriate, to make companies comply with environmental

---

[99] (...continued)
Laboratory. Internet home page. . Albuquerque, NM. January, 2003.

[100] NISAC. "Counter Terrorism." Los Alamos National Laboratory. Los Alamos, NM. April, 2002.

[101] Department of Homeland Security (DHS). *DHS Organization*. Internet web site. Washington, DC. May 29, 2003.

[102] DHS. Information Analysis and Infrastructure Protection Directorate (IAIP). Personal communication. June 9, 2003.

[103] Anonymous. "Shell, Olympic Socked for Pipeline Accident." *Energy Daily*. January 22, 2003.

and safety laws.[104] Along with other requirements, he asserted the department's intention to enforce laws that "call for facilities to develop emergency response plans" and that "assure that pipelines do not leak or explode."[105]

The Justice Department has not initiated any new pipeline cases since March. However, on April 1, 2003, DOJ and EPA did announce a $34 million civil penalty — the largest in EPA history — to Colonial Pipeline for seven recent oil spills. Along with other safety provisions, the penalty settlement requires Colonial to treat its entire 5,500 mile network as "high consequence" under OPS rules.[106] While there are currently few security-specific regulations in the federal code, high profile pipeline safety settlements do have security connections as noted earlier in this report. Moreover, they indicate DOJ's future willingness to enforce new security regulations that may arise from recent legislation.

Federal Energy Regulatory Commission

One area related to pipeline safety not under the OPS's primary jurisdiction is the siting approval of new gas pipelines, which is the responsibility of the Federal Energy Regulatory Commission (FERC). FERC's primary role is regulating prices for the transmission and sale of wholesale oil and natural gas in interstate commerce. But companies building interstate gas pipelines must first obtain from FERC certificates of public convenience and necessity. (FERC does not oversee oil pipeline construction.) FERC must also approve the abandonment of gas facility use and services. These approvals may include safety and security provisions with respect to pipeline routing, safety standards and other factors.[107] As a practical matter, however, FERC has traditionally left these considerations to the OPS.[108]

On September 14, 2001, the Federal Energy Regulatory Commission (FERC) notified FERC regulated companies that it would "approve applications proposing the recovery of prudently incurred costs necessary to further safeguard the nation's energy systems and infrastructure" in response to the terror attacks of 9/11. FERC also committed to "expedite the processing on a priority basis of any application that would specifically recover such costs from wholesale customers." Companies could propose a surcharge over currently existing rates or some other cost recovery method.[109] According to FERC, 3 pipeline operators have filed formal requests for

---

[104] Heilprin, John. "Ashcroft Promises Increased Enforcement of Environmental Laws for Homeland Security." Associated Press. *Washington Dateline*. Washington, DC. March 11, 2003.

[105] US Attorney General. "Prepared Remarks of Attorney General Ashcroft Meet and Greet with Environmental Press." Washington, DC. March 11, 2003.

[106] Anonymous. "US Reaches Landmark Settlement with Colonial Pipeline for Oil Spills in Five States." *Regulatory Intelligence Data.* Washington, DC. April 1, 2003.

[107] U.S. Code of Federal Regulations. 18 CFR 157.

[108] FERC. Personal communication. May 22, 2003.

[109] Federal Energy Regulatory Commission (FERC). News release. R-01-38. Washington, (continued...)

security cost recovery to date. Of these applications 2 were approved, 1 was withdrawn.[110]

On February 2003, FERC handed down a new rule (RM02-4-000) to protect critical energy infrastructure information (CEII). The rule defines CEII as information that "must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act." According to the rule, critical infrastructure is "existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters." CEII excludes "information that identifies the location of infrastructure." The rule also establishes procedures for the public to request and obtain such critical information, and applies both to proposed and existing infrastructure.[111]

On May 14, 2003, FERC handed down new rules (RM03-4) facilitating the restoration of pipelines after a terrorist attack. The rules allow owners of a damaged pipeline to use blanket certificate authority to immediately start rebuilding, regardless of project cost, even outside existing rights-of-way. Pipeline owners would still need to notify landowners and comply with environmental laws. Prior rules limited blanket authority to $17.5 million projects and 45-day advance notice.[112]

National Transportation Safety Board

Major pipeline incidents, like other transportation incidents, are investigated independently by the National Transportation Safety Board (NTSB). NTSB investigations would examine what caused an incident and whether it was accidental or deliberate. In this respect, NTSB could play a role in terror incident investigations. Since 1969, NTSB has investigated over 100 natural gas and oil pipeline incidents. Based on the probable cause of an incident, NTSB may make recommendations to prevent recurrences. NTSB may also conduct special studies of pipeline safety issues of national significance, and may evaluate the safety effectiveness of government agencies involved in transportation. For example, NTSB reviewed federal oversight of oil pipeline safety in 1996.[113] More recently, NTSB investigated both the Bellingham and Carlsbad pipeline accidents.

---

[109] (...continued)
DC. September 14, 2001.

[110] FERC. Personal communication. May 22, 2003.

[111] FERC. News release. R-03-08. Washington, DC. February 20, 2003.

[112] Schmollinger, Christian. "FERC OKs Emergency Reconstruction." *Natural Gas Week*. May 13, 2003.

[113] NTSB. *Evaluation of Accident Data and Federal Oversight of Petroleum Product Pipelines*. NTSB/SIR-96/02. Washington, DC. January 23, 1996.