

American Petroleum Institute Association of Oil Pipe Lines

Marty Matheson
General Manager, Pipelines
American Petroleum Institute
1220 L Street, NW
Washington, DC 20005
(202) 682-8192
(202) 682-8579 (fax)
matheson@api.org

Benjamin S. Cooper
Executive Director
Association of Oil Pipe Lines
1101 Vermont Avenue NW Suite 604
Washington, DC 20005
(202) 408-7970
(202) 408-7983 (fax)
bcooper@aopl.org

Security Planning and Preparedness in the Oil Pipeline Industry

August 2004

Almost three years have elapsed since the tragic events of September 11, 2001. The oil pipeline industry is committed to the integrity and security of the national oil pipeline network. We would like to take this opportunity to bring you up to date on oil pipeline industry security actions that have taken place since September 11, but focusing on recent months.

The oil pipeline network is a valuable national asset, which is owned, maintained and operated by private companies. Pipelines are the irreplaceable core of the U.S. petroleum transportation system and the means for both delivery of foreign and domestic crude oil to refineries and for moving finished products from refining and producing centers to consuming regions. Oil pipeline shipments account for 17% of all domestic freight moved nationwide, delivering more than 14 billion barrels (600 billion gallons) per year. The nation's oil pipeline network includes 160,000 miles of interstate transmission pipelines. Those pipelines are regulated from a safety and environmental perspective by the federal government through the U.S. Department of Transportation Office of Pipeline Safety.

Pipelines are physically robust. The vast majority of pipeline systems are underground and less vulnerable than aboveground facilities. Pipeline operators have been managing the integrity, safety and security of pipeline systems for many years. Most damage to pipelines can be readily repaired and pipeline operators have emergency response plans in place. Disruptions in supply can often be avoided by providing alternative forms of transportation for short periods or by using interconnections to move products around the site of damage to a pipeline.

Pipeline operators cooperated readily with the federal government to identify, for preparedness purposes, those pipeline facilities that are critical to the nation. Key critical pipeline assets have been identified using system risk analysis along with mutual discussion between operators and the Department of Homeland Security, the Department of Energy and the Department of Transportation. In addition to key critical assets, other pipeline systems may be considered viable terrorist targets or a release resulting from a terrorist attack from certain pipeline systems might have a significant impact on people,

on public drinking water, on regional energy supply, on military facilities important to national defense, or could potentially impact other modes of transportation or other critical infrastructures (electric power generation, telecommunications, or other utilities). These pipeline systems or portions of pipeline systems have also been specifically identified by operators. Information about critical assets forms a part of our nation's security and is not subject to public disclosure.

Security guidance for pipeline facilities is in place and pipeline operators are implementing that guidance for critical facilities. In April 2003, the American Petroleum Institute published "Security Guidelines for the Petroleum Industry" (second edition since 9/11) in close cooperation with the Department of Homeland Security, Information Analysis and Infrastructure Protection division. A third edition of the security guidelines will be published in Fall 2004. Part III of the guidelines specifically addresses hazardous liquid pipelines. By developing a pipeline security plan operators can improve the security of pipeline systems and develop the knowledge and processes for making security related decisions. Pipeline operators have and will continue to:

- Identify and analyze actual and potential events that can result in pipeline security related incidents
- Identify the likelihood and consequence of such events
- Provide an integrated means for examining and evaluating risks and selecting risk reduction actions
- Establish and track security plan effectiveness
- Establish security conditions (using the national threat advisory system) and specific protective measures based on the threat level

The security of pipeline facilities has to be evaluated in relationship to other energy assets. The guidelines are available from API free of charge at:

http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf

The federal government has established pipeline security contingency planning guidance, published that guidance for action by pipeline operators and asked that all pipeline operators submit a written statement concerning security preparedness. In September 2002, the U.S. Department of Transportation, in coordination with the Department of Energy and agencies that became the Department of Homeland Security, published a pipeline security information circular. The circular defined critical pipeline facilities identified appropriate measures for protecting critical facilities (based on the national threat advisory system) and defined a process by which the federal government would verify that operators had taken appropriate action and implemented satisfactory security procedures and plans. The information circular requested that operators submit a written statement confirming that the operator has:

- Reviewed the information circular and the Pipeline Security Contingency Planning Guidance
- Reviewed the consensus security guidance appropriate to its segment (oil or natural gas) of the pipeline industry
- Identified its critical facilities
- Developed a corporate security plan

- Begun implementing its corporate security plan to protect the physical and cyber security of its critical facilities

As of April 1, 2003, the U.S. Department of Transportation Office of Pipeline Safety has received certifications from operators of 95% of the U.S. oil pipeline infrastructure – more than 150,000 miles – regulated by the U.S. Department of Transportation. The companies that comprise the 95% are substantially all of the operators who operate large oil (both crude oil and refined products) pipeline systems in the United States, as well as many smaller operators. The remaining 5% include smaller pipeline operators or companies that are primarily in other businesses but may also have pipelines between plant facilities, may connect a manufacturing plant to a larger pipeline, or similar systems. The pipeline industry continues to recommend that all pipeline operators have security plans in place and certify to the federal government as requested by the U.S. DOT Office of Pipeline Safety. In addition to the mileage of pipelines regulated by the Department of Transportation, there are another 30-40,000 miles of small diameter, widely scattered oil pipelines servicing domestic production fields. These pipelines do not pose a security risk to energy facilities, energy supplies or to the public.

Beginning in April 2003 and continuing, the U.S. Department of Transportation and the Department of Homeland Security, Transportation Security Administration are conducting verification checks at pipeline companies to validate the certifications made by pipeline operators. The U.S. Department of Transportation Office of Pipeline Safety is the federal agency responsible for providing oversight for oil and natural gas pipelines. The Office of Pipeline Safety has a trained inspection force in place, which has been conducting safety and environmental audits and inspections of pipeline systems for many years. OPS inspectors operate out of five regional offices and are very familiar with the pipeline operations within and across the regions. The Transportation Security Administration and the Office of Pipeline Safety have prepared a set of protocols for validating pipeline security preparedness and are conducting verification checks. To date 33 natural gas and hazardous liquid transmission pipeline companies have been reviewed by TSA.

Pipeline operators are conducting and will continue to conduct vulnerability assessments of critical pipeline facilities as the federal government and the pipeline industry develop a better understanding of terrorist threats and terrorist capabilities. Prior to September 11, 2001, the federal government did not provide guidance nor recommend the need for private industries, such as the energy industry, to conduct vulnerability assessments based on terrorist threats. Many petroleum companies operating globally have had experience planning to prevent terrorists or other criminals from breaching their facilities and committing crimes, including the release of petroleum products or the damaging of facilities and potentially the communities around those facilities. Since 9/11, knowledge from companies operating overseas, from federal agencies responsible for nuclear plants and military facilities, and from security services (the FBI and private security companies) has been mined to provide guidance to domestic pipeline and other energy companies on conducting vulnerability assessments. The national laboratories (National Energy Technology Lab and Sandia) housed in the

Department of Energy have made guidance and experts available to the energy industry. Pipeline operators have conducted vulnerability assessments or participated in vulnerability assessments of larger manufacturing or port facilities encompassing multiple operators, industries, and transportation modes.

A new methodology for assessing the vulnerabilities of petroleum industry operations has been developed in cooperation with the Department of Homeland Security. Vulnerability assessments must encompass specific facilities as well as the supply chain for the distribution of petroleum products. “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industry,” published by API in May 2003, provides guidance to operators and encompasses the recommendations and concerns of the DHS Information Analysis and Infrastructure Protection division. The methodology has been accepted and endorsed by the Department of Homeland Security. A new edition of this methodology will be released in the Fall 2004. The methodology is available from API free of charge at:

http://api-ec.api.org/filelibrary/SVA_2003.pdf

The pipeline industry is now developing an industry standard for the protection of control functions and Supervisory Control and Data Acquisitions Systems (SCADA). In addition to the focus on the physical security of pipeline facilities, the industry is also evaluating the potential vulnerabilities of information technology systems, process control and data exchange from the pipeline to the control center. The industry has conducted a review of the SCADA standards for other industries and is now drafting a SCADA security standard for pipelines. API anticipates that this new standard will be published in the Fall 2004.

Security actions have taken many forms depending on the specific circumstances an operator faces with a particular pipeline system, the critical nature of the services, and the current level of threat warning issued by the federal government. Provided here is a sampling of the types of actions, other than planning and awareness, which operators have taken, are taking or will take as circumstances dictate. Pipeline operator security plans are in place. Employees have been provided with information and techniques to improve their awareness of the potential for terrorist or criminal acts. Awareness is the single most important aspect of preparedness. It is helpful to understand some of the other types of actions pipeline operators have taken. Some of these actions have taken place at many facilities, some are specific to critical facilities, and some are taken only as the threat level increases. The following are some examples of actions taken to give readers a sense of the oil pipeline industry’s preparedness. Pipeline operators have --

- Direct relationships, including telephone contact and face-to-face meetings, with FBI regional field personnel.
- Joined FBI Infraguard program
- Established inter-company cooperative efforts for specific locations
- Obtained “secret” level security clearances for selected operational personnel to ensure that threat information can be communicated directly under circumstances when such discussions are warranted

- Joined government-industry threat information dissemination services, including the Energy Information Sharing and Analysis Center (ISAC)
- Installed surveillance cameras at certain facilities
- Installed physical barriers to entrances to certain facilities
- Conducted response drills using terrorist scenarios as a basis for training personnel and working with new federal partners including law enforcement and the FBI under emergency circumstances
- Used guard patrols at certain facilities under certain threat conditions
- Limited access to facilities and entrance only after positive identification

The pipeline industry and the petroleum industry have been conducting informational briefings on how pipeline systems function to ensure that government agencies and intelligence personnel understand the services provided, the potential risks and vulnerabilities, and what pipeline operators are doing to improve security.

The pipeline industry has recognized that it is crucial for those that are evaluating intelligence information to understand the infrastructures they are working to protect. The pipeline industry and individual pipeline companies have briefed officials at the Department of Homeland Security, the Transportation Security Administration, the DOT Office of Pipeline Safety, the U.S. Coast Guard, the Occupational Health and Safety Administration, the Environmental Protection Agency, the Department of Energy, the National Institute for Standards and Technology, the staff of Congressional Committees charged with oversight of security agencies, and intelligence personnel from various federal agencies. This industry will continue to take advantage of opportunities to provide such informational briefings.

The oil pipeline industry is committed to pipeline safety, to environmental protection and to providing reliable pipeline transportation services. The oil pipeline industry has plans in place to assure pipeline security to the extent that is practical and reasonable. Oil pipeline operators have taken prudent protective actions and will continue to analyze vulnerabilities of pipeline systems. Pipeline operators will be continuously monitoring threat information that is provided by federal, state and local law enforcement agencies. The pipeline industry will continue to work cooperatively with the Department of Homeland Security, the Transportation Security Administration, the DOT Office of Pipeline Safety and the intelligence community.