



HUNTON & WILLIAMS LLP
1900 K STREET, N.W.
WASHINGTON, D.C. 20006-1109

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

STEVEN P. SOLOW
DIRECT DIAL: 202-419-2065
EMAIL: ssolow@hunton.com

FILE NO:

March 1, 2004

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, DC 20002

Dear Commissioners:

This letter is sent on behalf of the Association of Oil Pipelines (AOPL). The AOPL writes in response to the Commission's request for comments regarding possible revisions to the guideline treatment for the illegal transportation of hazardous materials.

The AOPL is an unincorporated nonprofit organization started in 1947. AOPL represents 49 common carrier oil pipeline companies. AOPL members carry nearly 80% of the crude oil and refined petroleum products moved by pipeline in the United States. Among other things, the AOPL represents its members on legislative and regulatory matters and in the federal courts.

The Commission has sought comments in response to the August 1, 2003 Department of Justice submission which alleges that the sentencing guideline applicable for hazardous materials, § 2Q1.2 is not adequately suited to illegal transportation of hazardous materials. The Department of Justice suggests two grounds to justify changes to the guidelines: first, that illegal transportation of hazardous material is different from typical pollution offenses covered by § 2Q1.2 and has characteristics not addressed by that guideline; and, second, that the specific offense characteristics set forth in § 2Q1.2 are not characteristic of illegal transportation of hazardous materials. For the reasons set forth below, the AOPL urges the Commission to reject the structure of the Department's approach and offers an alternative approach more closely tailored to the stated need.

The AOPL supports the Department's effort to obtain enhancement of penalties where hazardous materials and/or the hazardous material transportation infrastructure are used to commit (or attempt to commit) acts of terrorism. As described in the attached summary of

United States Sentencing Commission

March 1, 2004

Page 2

industry security efforts¹, the pipeline industry has entered into close cooperation with federal law enforcement and regulatory agencies to address shared concerns about the integrity and security of the nation's critical private infrastructure. In addition, the AOPL support the Department's effort to obtain enhancement of penalties where violations involve controlled substance manufacturing or trafficking offenses.

As set forth below, there are existing provisions of the Guidelines that address the potential misuse of the nation's hazmat transportation infrastructure as a weapon. To the extent further revision is considered appropriate, there is precedent within the guidelines for a much more straightforward approach to this issue.

To address "one-time, catastrophic occurrences," involving illegal hazardous materials transportation by terrorists, the guidelines already provide for a "victim related enhancement" at § 3A1.4 for crimes which involved or were intended to promote terrorism.

If further revision is thought to be necessary, a direct and simple precedent is found in § 2B1.1(b)(12)(B)(i) which provides for a specific offense characteristic in crimes involving theft and embezzlement if:

the offense (i) substantially jeopardized the safety and soundness of a financial institution . . .²

Using this model to address illegal hazardous material transportation by those with the intent to commit acts of terrorism, or to engage in controlled substance manufacturing or trafficking offenses, the guidelines could add a new specific offense characteristic to § 2Q1.2 as follows:

(7) If the offense: (i) involved, or was intended to promote a federal crime of terrorism, increase by 12 levels; but if the resulting offense level is less than level 32, increase to level 32; (ii) involved, or was intended to promote a controlled substance manufacturing or trafficking offense, increase by 2 levels, but if the resulting offense level is less than level 14, increase to level 14.

¹ See Attachment 1, "Security Planning and Preparedness in the Oil Pipeline Industry," API-AOPL Environmental and Safety Initiative, August, 2003, available at: <http://www.aopl.org/pubs/reports.html>.

² United States Sentencing Guidelines, § 2b1.1(b)(12)(B)(i) (January, 2003).

This would provide additional specific offense characteristics that would be consistent with the model utilized in § 2B1.1, and with the language for victim-related adjustments for crimes involving terrorism in § 3A1.4 and for transportation offenses involving drugs in § 2D1.12(a)(12) and (b).

The Department correctly notes that § 2Q1.2 was not originally designed to cover hazardous material transportation violations. However, as the Department also notes, since 1993, hazmat crimes were added to § 2Q1.2.

Thus, illegal transportation of hazardous material *is* covered by § 2Q1.2.³ Further, almost all of the offense characteristics proposed for comment for illegal transportation of hazardous material are covered by the existing guidelines. Thus, a violation of the legal limits on hazardous material transportation results in a base offense level of 8. If there is a release, a four-level enhancement may apply, and if there is a related evacuation or disruption of public utilities or a significant clean up, then another four-level enhancement would apply. Should the offense result in a substantial likelihood of death or serious bodily injury, a nine-level enhancement would apply.⁴ The Department has long noted that these sanctions available under § 2Q1.2 provide serious punishments for environmental violations.

Moreover, the use of criminal enforcement of environmental laws has proceeded step-wise, with criminal enforcement following the gradual clarification of regulatory requirements and as a support and enhancement to the government's other enforcement tools of administrative and civil enforcement.

In that context, it should be considered that hazardous material transportation regulation is in a remarkable state of change. In response to 9/11, new partnerships have developed between the private sector and federal, state and local governments to devise the means to identify the areas of greatest potential risk and develop the strategies most likely to address those risks. To the extent that the Department's proposal seeks to increase penalties as a means of reducing those risks, the effort is premature, as the government itself is still determining what acts (or failures

³ United States Sentencing Guidelines, Appendix A (November 2002) Listing Statutory Provisions found at title 49.

⁴ Of course other enhancements could apply as well, such as those dealing with the offenders role in the offense in Chapter 3B and for acts of obstruction under 3C.

United States Sentencing Commission
March 1, 2004
Page 4

to act) in the area of hazardous material transportation constitute the greatest potential risk (and which therefore might receive greater sanctions should they be violated).⁵

A recent Congressional Research Service Report for Congress noted that after the terrorist attacks:

Pipeline operators reviewed procedures, tightened security, rerouted transportation patterns, closely monitored visitors and made capital improvements to harden key facilities. The Association of Oil Pipelines (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.⁶

Ninety-five percent of AOPL operators had developed new security plans and instituted appropriate security procedures by February 2003. Pipeline operators have joined with the Department Homeland Security to establish a cooperative, industry-directed database to provide real-time threat alerts, cyber alerts and solutions. AOPL members have also worked with the Department of Homeland Security to identify critical facilities that warrant government protection should they be threatened and have responded to requests by the DOT's Office of Pipeline Safety and DHS's Transportation Security Administration to conduct vulnerability assessments. These are only a few of the ways that the AOPL and its members have moved to respond to security threats and to increase government-industry partnerships to enhance the protection of the nation's critical infrastructure. These efforts to identify risks and problems in the hazardous material transportation industry are still in process.

In the context of these efforts, most of the suggested revisions to § 2Q1.2 are not focused on the utility of this guideline provision as a means of addressing national security threats or drug trafficking. Guidelines revisions have generally flowed from the careful study of empirical information. Outside of the approach noted above to address acts of terrorism against our nation's critical private infrastructure or drug related offenses, the small number of criminal

⁵ For example, in a proposed rulemaking, the DOT and the Transportation Security Administration are evaluating the need to require further security enhancements on materials or categories of materials that present the most serious security risks in transportation. 68 Fed. Reg. 37,470, 34,477 (June 9, 2003).

⁶ CRS Report for Congress, "Pipeline Security: An Overview of Federal Activities and Current Policy Issues," updated February 5, 2004, p. CRS-11.

United States Sentencing Commission

March 1, 2004

Page 5

hazmat cases do not provide a basis for the non-security focused proposals on § 2Q1.2. There is simply too little "additional information and . . . firm empirical basis" which the Commission itself considers a necessary basis for revisions to the guidelines.⁷

* * *

While not the main focus of these comments, the reference to possible changes to the Chapter Eight guidelines to specifically cover hazmat compliance appears to conflict with the past design of Chapter Eight and the Commission's current proposal to revise Chapter Eight. As the Commission is well aware, Chapter Eight provides leniency for effective programs to prevent and detect violations of law. Chapter 8 has long served an outsize role in determining the shape and content of corporate compliance plans. Following the October 2003 report of the Ad Hoc Advisory Group on the Organizational Sentencing Guidelines, the Commission has published proposed amendments to Chapter Eight which propose a new standalone guideline focused on compliance programs.

The provisions of the Chapter Eight guidelines that address compliance programs have been crafted to have broad application. Notably, some concerns over the proposed changes focus on whether or not expanding the specificity of the definition of an effective compliance program is beyond the Committee's purview or expertise. This concern would be amplified should the Commission begin developing industry specific criteria. What is considered to be the most effective compliance program for a given industry is subject to a vast number of economic, technological and other factors. It would undermine the broad impact of the Chapter Eight guidelines in this area should the Commission attempt to make such narrow prescriptions.

* * *

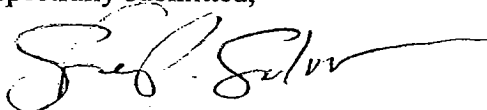
The AOPL hopes that these comments are useful to the Commission. The AOPL would appreciate the opportunity to send a representative to testify before the Commission's public hearing on March 17, 2004.

⁷ United States Sentencing Commission, Guidelines Manual, Chapter 1, Part A, Introduction and General Application Principles, "A Concluding Note."

**HUNTON &
WILLIAMS**

United States Sentencing Commission
March 1, 2004
Page 6

Respectfully submitted,

A handwritten signature in cursive script, appearing to read "S. P. Solow", with a long horizontal flourish extending to the right.

Steven P. Solow

SPS/kmm

cc: Lisa Rich, Esq.
Staff Counsel, United States Sentencing Commission

[1-111]

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 2003

Almost two 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 July 2002, the American Petroleum Institute published "Guidelines for Developing and Implementing Security Plans for Petroleum 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 also been considered in relationship to other energy assets. The petroleum industry as a whole has published, "Security Guidance for the Petroleum Industry" (April 2003) in close cooperation with the Department of Homeland Security, Information Analysis and Infrastructure Protection division.

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 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 this past April 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. Five pipeline operators have been reviewed as of August 2003 and approximately 30 of the largest operators will be reviewed by the end of 2003.

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. "Vulnerability Assessment for the Petroleum 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 is being evaluated by the U.S. Coast Guard for use in petroleum facilities associated with U.S. ports.

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.

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 Infragard 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 API and 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 cooperative with the Department of Homeland Security, the Transportation Security Administration, the DOT Office of Pipeline Safety and the intelligence community.