SECURITY POLICY CONSIDERATIONS FOR INLAND FACILITIES AND PIPELINES

Gary Yoshioka and Ellinor Coder
ICF Consulting, 9300 Lee Highway, Fairfax VA 22031

ABSTRACT

Although facilities in the United States have not been subject to major oil spills caused by intentional acts, around the world acts of war and terrorism account for a large fraction of reported major oil spills. The Oil Pollution Act of 1990 requires response plans that address a "worst case discharge;" however, the implementing regulatory agencies did not foresee the possibility of deliberate attacks that could involve multiple storage tanks or several pipeline response zones. In addition, the terrorist attacks of September 11, 2001 highlighted the problems with the current U.S. federal response and contingency plans.

The U.S. Coast Guard published a rule that requires operators of marine-transportation-related oil facilities to implement a variety of security measures. Inland facilities and pipelines are generally exempt from the security regulations; nevertheless, those facilities and pipelines can take steps to increase their own security preparedness by emulating the Coast Guard provisions. Homeland Security Presidential Directive HSPD-7, issued on December 17, 2003, identified critical infrastructure sectors and sector-specific agencies to facilitate vulnerability assessments of the sectors. The U.S. Department of Energy is responsible for coordinating the protection of critical infrastructures in the Energy Sector, which includes the production, refining, storage, and distribution of oil.

In this paper, we discuss recent trends in Federal requirements and current provisions for oil industry security planning. We highlight types of major oil facilities that need to consider the possibility of a terrorist attack, as well as recommendations by industry groups. We conclude with suggested areas for industry planning improvement.

INTRODUCTION

The hazardous nature of many oil products, the large quantities of these products that are often transported or stored on-site, and our daily dependence on oil products make this industry an attractive terrorist target. Attacks on petroleum facilities in Iraq and other countries underscore warnings from the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) that the threat of a terrorist attack on U.S. oil facilities is more serious than ever before. Safeguarding the U.S. energy sector has become a national priority, and the U.S. Environmental Protection Agency (EPA) is taking proactive steps to re-evaluate existing regulatory programs in order to create a uniform set of threat deterrence guidelines for the oil industry.

In January 2004, the Democrats on the House Select Committee on Homeland Security released the initial findings of a report—*America At Risk: The State of Homeland Security*—that alleged gaps in the Bush Administration's homeland security efforts. One finding emphasized lax chemical plant security and noted that there are more than 66,000 chemical facilities in U.S. cities, towns, and rural areas. Oil storage facilities, however, number in the hundreds of thousands and can be even more vulnerable to terrorists than chemical facilities.

DISCUSSION

International incidents

Around the world, war and acts of terrorism account for a large fraction of major oil spills, as highlighted in Table 1. Terrorist acts caused hundreds of major pipeline spills in recent years. For example, of the 257 largest oil spills in 1999, more were caused by terrorist bombings in Colombia alone (51) than the combined number of spills from tankers, barges, and other vessels worldwide (36), according to data published by Cutter Information Corp. (DeCola 2000). Between 1986 and 2001, leftist guerrillas bombed Colombia's Cao Limon oil pipeline nearly 900 times, an average of once every six days. Two war-related oil spills in the Persian Gulf are among the largest ever to occur—the 1983 Nowruz No. 3 well spill during the Iraq-Iran War and the 1991 Sea Island installation spill during the Gulf War. Each of these was several times larger than the Exxon Valdez spill.

Threats to oil facilities have increased drastically. In April of 2004, terrorists attempting to damage Iraqi infrastructure attacked Arabian Gulf oil terminals in Bahrain. Islamic militants attacked oil complexes and residential compounds in Saudi Arabia in May, killing or capturing several petroleum industry workers. Pipeline bombings in Iraq in June halted oil exports as insurgents stepped up attacks prior to the change in government. In August, saboteurs damaged oil pipelines at separate sites in Iraq's northern and southern regions, and insurgents gunned down an officer with the State-run oil company. The saboteurs drilled holes in the southern line, and an explosion damaged the northern line. Insurgents frequently target Iraq's oil infrastructure to undermine the new government's reconstruction efforts, which depend largely on oil revenue.

Recent trends in U.S. energy security policy

The Homeland Security Act of 2002 established the U.S. Department of Homeland Security (DHS), an executive level Federal agency whose missions are to prevent terrorist attacks, reduce vulnerability to attacks, and assist in the recovery from attacks. DHS serves as a cross-sector coordinator to facilitate cooperation among all levels of government and with the private sector to achieve its goals.

On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which identified 17 critical infrastructure sectors and designated sector-specific

Table 1: Security incidents at international oil facilities:

Date	Security Incident	Impact
1983	Nowruz No. 3 well spill during the Iraq-Iran War	80 million gallons of oil are spilled
1998	Saudi oil facilities bombed	Fueled conflict between Iran and Saudi Arabia over Muslim pilgrimage to Mecca; several Saudi Shia are executed
1991	Sea Island installation spill during the first Gulf War	240 million gallons of oil are spilled
1998	A pipeline jointly owned by the Columbian State Oil Company, Ecopetrol, and U.S., French, Canadian, and British companies is bombed by the National Liberation Army	71 people killed, 100 more injured
1999	Armed youths storm a Shell oil platform in Nigeria	3 persons kidnapped and an undetermined amount of damage to the platform; other oil seizures followed in Nigeria.
1999	Terrorist bombings cause 51 spills in Columbia	
2002	Al-Quaida suspected of ramming the French oil tanker, *Limberg*, with an explosive-laden boat	One person killed, 4 more wounded
2004	Terrorists attack Arabian Gulf oil terminals in Bahrain, militants attack oil complexes in Saudi Arabia, and pipelines are bombed in Iraq	Exports of oil are halted, damage to pipelines are intended to undermine oil revenues used for reconstruction in Iraq

agencies to facilitate vulnerability assessments of each sector. HSPD-7 calls for the Department of Homeland Security to oversee the creation of the National Infrastructure Protection Plan (NIPP) to collect and integrate each sector's critical infrastructure protection plan, or Sector Specific Plan (SSP). HSPD-7 designates Energy as one of the 17 sectors in the NIPP, and the U.S. Department of Energy is responsible for coordinating the protection of critical infrastructures in the Energy Sector. Energy includes both the electricity industry and the oil and natural gas industry. The oil industry includes the production, refining, storage, and distribution of oil.

An Energy SSP would identify processes for determining the sector's infrastructure and asset vulnerabilities. By assessing the sector's security vulnerabilities, the industry can develop specific objectives to reduce those vulnerabilities. Because the Energy sector supports other sectors and facilities critical to national security, a disruption has the potential to affect essential services. As a result of the vulnerabilities in the sector, the Department of Energy is facilitating cooperation between different levels of government, as well as between the government and the private sector, to define roles in securing the Energy sector's critical infrastructure. One example is the creation of the Energy Information Sharing and Analysis Center, described below.

Industry security planning

There are several models in place currently that provide information that is helpful in identifying the types of regulatory changes that will address security threats at inland oil facilities. As described below, current EPA Oil Program rules for non-transportation-related facilities establish baseline regulatory security policies. Recent security measures required by the Maritime Transportation Security Act of 2002 (MTSA) also provide guidance to inland facilities, as MTSA requires a variety of security measures for coastal oil facilities. Finally, the National Petroleum Council and the American Petroleum Institute provide some security guidance to the industry.

Current EPA Oil Program Rules

In the United States, under the Clean Water Act and the Oil Pollution Act of 1990, EPA promulgates regulatory provisions for non-transportation-related facilities that handle, store, or transport oil. These rules include Spill Prevention Control and Countermeasure (SPCC) Plan requirements for oil facilities with more than 1,320 gallons of aboveground storage capacity, and Facility Response Plan (FRP) requirements for larger facilities from which a spill may cause substantial harm to the environment. A facility must prepare an FRP if: (1) it transfers oil over water to or from vessels and has an oil storage capacity of 42,000 gallons or more, or (2) it has an oil storage capacity or one million gallons or more and meets at least one of four other facility characteristics related to proximity to sensitive environments or drinking water intakes, spill history, and lack of secondary containment.

These EPA Oil Program regulations contain some security provisions, but at the time the regulations were first developed, the focus was on preventing vandalism and responding to accidental storage tank failure. Nonetheless, the SPCC provisions in 40 CFR part 112 require prevention planning for oil discharges of all types, whether the cause is accidental, a natural hazard (such as an earthquake or lightning), or deliberate (such as vandalism or terrorism). EPA's FRP requirements address responses to worst case discharges from facilities such as refineries, tank farms, or terminals. Such discharges can damage the facility, disrupt waterborne commerce, and cause substantial economic or environmental damage, which are consequences that terrorism security measures are designed to prevent.

In Part 112, the FRP must describe facility security, as appropriate, including enclosures such as fencing, guards and their duties, and lighting. The SPCC Plan provisions specify that lighting should be adequate to prevent discharges caused by vandalism and that oil storage areas must be fully fenced with entrance gates locked or guarded when the facility is unattended. The FRP includes a detailed site plan diagram, hazard evaluation, and vulnerability assessment. The assessment in the FRP examines

outcomes and potential effects of an oil spill incident, such as the shutdown of downstream water intakes. The FRP provisions require drills and exercises, including evaluations, and logs and records must be submitted to EPA as part of the FRP. The requirements may be met by following the National Preparedness for Response Exercise Program (PREP) guidelines, which provide for internal exercises including notification drills and spill management team tabletop exercises, as well as external exercises such as government/industry area exercises. Under the authority of the Clean Water Act, EPA periodically conducts announced and unannounced drills for facilities with FRPs.

Maritime Transportation Security Act (MTSA) Rules

The United States Coast Guard (USCG) security rules are particularly relevant to EPA-regulated facilities, because some of those facilities that transfer oil in bulk to or from a vessel are subject to the MTSA requirements for facilities. Others may be subject to an Area Maritime Security Plan developed under the USCG rules implementing the MTSA or may be directed by the USCG Captain of the Port to implement security measures. The MTSA required the USCG to conduct facility and vessel vulnerability assessments to identify those facilities and vessels at high risk of being involved in a transportation security incident. The MTSA also mandated that high-risk ports, facilities, and vessels conduct vulnerability assessments and have security plans approved by the USCG to address those vulnerabilities that are identified. On October 22, 2003, the USCG published a series of final rules to promulgate the maritime security requirements mandated by the MTSA.

Under the USCG rules, the owner or operator of a facility will have to conduct a Facility Security Assessment, develop a Facility Security Plan (FSP), and implement certain security measures and procedures. To comply with the regulations, facility owners and operators must:

- Designate a Facility Security Officer (FSO), who will have security duties to fulfill;
- Assign the FSO to ensure that a Facility Security Assessment is conducted and a report is prepared;
- Develop and submit for approval an FSP, which will be valid for five years from the date of approval but must be audited annually by the Facility Security Officer. (The submission deadline was December 31, 2003.) However, the personnel performing an audit of the FSP must not have regularly assigned security duty at the facility, meaning the FSO cannot audit the FSP.
- Operate the facility in accordance with the approved plan;
- Regularly conduct security drills and exercises. Owners and operators must conduct an exercise at least once each calendar year, with no longer than 18 months between exercises, and at least one drill every 3 months. These security exercises may be part of a cooperative exercise program or may be combined with other required exercises.
- Implement any additional security measures required by changes in Maritime Security (MARSEC) Level, which reflects the prevailing threat environment to the marine elements of the national transportation system;
- Report all security breaches and security incidents; and
- Coordinate shore leave for vessel personnel or crew change-out, and coordinate visitor access through the facility to the vessel (including representatives of seafarers' welfare and labor organizations) in advance of a vessel's arrival.

Table 2 compares the EPA's SPCC and FRP requirements with those of the FSP required by the Coast Guard.

National Petroleum Council Recommendations

Even before the events of September 11, 2001, the National Petroleum Council addressed critical infrastructure protection in the oil and gas sector, particularly for pipelines. The 2001 Council report emphasized the importance of protecting cyber systems because of the sector's growing dependence on electronic communications. Individuals and groups, from hackers to organized terrorists, have the ability to simultaneously attack multiple sites. Among the report's major recommendations are the following:

- Companies in the oil and gas industry should conduct vulnerability assessments of their systems and operations, both physical and electronic, and take action as appropriate;
- Companies should enhance their response and recovery plans as they relate to information technology system disruptions, while maintaining and implementing plans for disruptions to physical facilities;

Table 2: Comparison of EPA FRP and U.S. Coast Guard FSP Requirements

	EPA FRP Requirements	U.S. Coast Guard FSP Requirements
Assessment	The FRP includes a detailed site plan diagram, and emergency response action plan, hazard evaluation, and vulnerability analysis.	The FSP is based on a Facility Security Assessment.
Fencing, lighting, and monitoring	The FRP must describe facility security, including enclosures such as fencing, guards and their duties, and lighting.	The FSP must specify the required security measures to continuously monitor the facility through a combination of lighting, security guards, and other methods.
Notification	The FRP must include an emergency phone list, with contact information for the National Response Center and emergency response personnel.	Security incidents are reported to the National Response Center and to emergency responders. Communication systems and procedures must allow contact with national and local authorities.
Evacuation	The FRP requires detailed evacuation plans for the facility in case of a discharge.	The owner or operator must ensure that security personnel are able to evacuate the facility in case of security threats.

- The industry should establish a secure information-sharing mechanism to collect information on physical and electronic threats, certain vulnerabilities, incidents, and solutions/best practices.

American Petroleum Institute (API) Security Guidelines

The American Petroleum Institute, in collaboration with the Department of Homeland Security, published two guidance documents for the petroleum industry: "Security Guidance for the Petroleum Industry (2002)," and "Security Vulnerability Assessment for the Petroleum and Petrochemical Industries (2003)." API recommends all member facilities perform a formal risk-based Security Vulnerability Assessment for their facility. Elements of the assessment include facility characterization, threat identification and assessment, identification of potential security-related events or conditions that pose a threat, assessing the risk of these elements and ranking that risk, as well as identifying and evaluating risk mitigation options. The API encourages facilities to include a variety of aspects in their security plan, including communications, cyber security, periodic re-evaluation of security measures, incident reporting and investigation procedures, and emergency response and management programs. Suggested threat deterrence methods are also correlated to increasing threat level. The API lists resources and guidance with which each sub-sector within the petroleum industry can create its own comprehensive security management plan and Security Vulnerability Assessment. The API also provides extensive guidance on cyber security measures.

Energy sector organizations can share threat information and deterrence solutions through the Energy Information Sharing and Analysis Center (ISAC), a secure Internet site maintained by the API. The Center contains analytic tools, a centralized repository of threat information gathered from various government agencies, and other assets. The ISAC is designed to create a mechanism for industry stakeholders to share security and vulnerability information relevant to the energy sector, including solutions to vulnerabilities identified by private stakeholders. Government agencies, including law enforcement and regulatory bodies, will not have access to the ISAC in order to encourage the free exchange of information.

Implications for Response Planning

The Federal Response Plan developed in 1992 recently has been modified to include a Terrorism Incident Annex to outline how the Federal Government will support state and local governments in response to terrorist incidents. Several states have groups or task forces addressing planning and preparedness activities at the state and local levels. DHS is preparing the National Response Plan, which will replace the Federal Response Plan to implement domestic incident management authorities, roles, and responsibilities of the Secretary of Homeland Security, and to provide one unified plan for the Federal government's response to acts of terrorism, major disasters, and other emergencies. A final draft of the National Response Plan was issued in June 2004.

Many Area Contingency Plans developed pursuant to OPA 90 have been or are in the process of being revised to address acts of terrorism. The plans include provisions on defining agency roles and responsibilities and on coordinating with other public and private sector plans. Preventing terrorist threats is primarily a law enforcement function but consequence management measures to protect public health and safety are the responsibility of states and the Federal government.

CONCLUSIONS

In order to improve industry preparedness for security threats, there are a number of options that regulatory agencies overseeing inland oil facilities and pipelines should consider:

- Agencies could expand the applicability of spill prevention and response provisions to include security and terrorism issues. For example, the duties of the Qualified Individual in the FRP rule can be expanded to include the duties of a Facility Security Officer. The vulnerability assessment required by the FRP can examine the facility's vulnerability to a security breach. Security drills and exercises can be incorporated into the current program of required drills and exercises.
- Facilities and pipelines could conduct Facility Security Assessments and develop Facility Security Plans. Certain security measures can vary by threat level, just as security at maritime facilities varies by MARSEC levels. Like the USCG rule, a revised SPCC rule can emphasize access control, scheduling of oil transfers, and coordination with transport vehicles and pipelines.
- Regulatory agencies could propose that relevant suggestions from the National Petroleum Council and American Petroleum Institute be adopted. Industry guidance documents contain detailed recommendations about access control measures, perimeter protection, transportation nodes, cyber security, employment practices, vulnerability assessments, communications, information sharing, and training topics. A proposed rule could include some of these detailed provisions, reference existing industry guidance, or solicit comments on appropriate regulatory language.
- Agencies could require coordination with other plans. Any rule for facilities or pipelines must be consistent with the requirements of the National Response Plan and must recognize the new provisions of Area Contingency Plans, port security plans, and state plans.

REFERENCES

American Petroleum Institute, 2002. Security Guidance for the Petroleum Industry.

American Petroleum Institute, 2003. Security Vulnerability Assessment for the Petroleum and Petrochemical Industries.

DeCola, E., 2000. International Oil Spill Statistics: 1999, Cutter Information Corp., Arlington, MA.

National Petroleum Council, 2001. Securing Oil and Natural Gas Infrastructures in the New Economy, Committee on Critical Infrastructure Protection.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003. White House.

BIOGRAPHY

Gary Yoshioka, a project manager in the Emergency Management and Homeland Security Practice at ICF Consulting, has more than 25 years experience specializing in environmental regulatory analysis. He has provided consulting services to the U.S Environmental Protection Agency in the development of every major rulemaking on oil spill prevention planning and hazardous substance release reporting since 1985. He holds a J.D. from the University of Maryland School of Law and a Ph.D. in Geography and Environmental Engineering from the Johns Hopkins University.