

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Transportation Security Administration  
Office of Intelligence

# Pipeline Threat Assessment



23 October 2008



**Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized TSA official. No portion of this report should be furnished to the media, either in written or verbal form.

# (U) SCOPE



**(U//FOUO)** The Transportation Security Administration's (TSA) mission includes enhancing the security preparedness of our nation's hazardous liquid and natural gas pipeline systems. This 2008 threat assessment addresses terrorist attacks against oil and gas pipeline facilities overseas and considers the potential for attacks against the oil and gas pipeline industry in the United States.

**(U//FOUO)** Pipelines are a mode of transportation with distinct characteristics and security requirements. Pipelines operate in all 50 states and transport more than two-thirds of all petroleum products, including gasoline, diesel and jet fuel, home heating oil, kerosene, and propane. Natural gas transmission and distribution pipelines transport natural gas from sources to residential, commercial, and industrial customers. Hazardous liquid pipelines transport crude oil to refineries and refined oil products to product terminals and airports. America depends daily on its pipelines to meet its oil and gas requirements.

**(U)** *Virtually the entire U.S. pipeline system and critical infrastructure is owned and operated by private entities. The U.S. pipeline system is comprised of 161,189 miles of liquid pipelines with more than 200 operators; 309,503 miles of natural gas transmission pipelines with more than 700 operators; and 1.9 million miles of natural gas distribution pipelines with more than 1,300 operators.*

# (U) EXECUTIVE SUMMARY

*(U//FOUO) At this time, there is no credible information regarding specific plans by terrorist groups or domestic extremists to conduct an attack on the U.S. pipeline network. TSA's Office of Intelligence (TSA-OI) assesses, however, that the U.S. system and its related infrastructure remain an attractive target to both terrorists and domestic extremists alike, as long stretches of open unattended pipeline are difficult to protect and the economic impact of attacks would be significant.*

*(U//FOUO) Al-Qa'ida, in particular, has noted the potentially damaging impact pipeline attacks—both in the United States and abroad—would have on the Homeland's economy, national security, and public health and psychology. Al-Qa'ida's demonstrated capability and intent to target oil and gas infrastructure overseas, and the group's desire to continue attacks in the Homeland, suggest similar attacks could occur inside the United States.<sup>1</sup>*

## (U) Key Findings

- *(U//FOUO) Transnational terrorist groups, such as Al-Qa'ida, pose the primary threat to the U.S. pipeline network. Single-issue extremist groups, industry insiders, and lone wolves may also pose a threat to the pipeline system.*
- *(U//FOUO) The interdependency of pipeline infrastructure with oil refineries, tank farms, and distribution centers increases the likelihood that the overall shared infrastructure will be impacted in the event of an attack.*
- *(U//FOUO) Improvised explosive devices have been the preferred method of attack against gas and oil facilities worldwide. Vehicle-borne improvised explosive devices have also been a successful method of attack against pipelines and oil facilities. Pipeline control systems are also vulnerable to cyber attacks, although we have no indications that terrorists pose a threat to Supervisory Control and Data Acquisition supporting pipelines.*
- *(U//FOUO) U.S- or Western-owned/operated pipelines in foreign countries are at increased risk of attack by Islamic extremists who oppose a foreign presence or who see a foreign presence as an embezzlement of natural resources.*
- *(U//FOUO) Suspicious incidents involving photography and surveillance of pipeline infrastructure in the Homeland are of particular concern. Reporting such incidents can help law enforcement and homeland security officials identify unusual behavior, trends, patterns, as well as possible criminal acts or potential malicious interests or intent.*



# (U) TSA-OI THREAT ASSESSMENT

## (U) Threat Overview

(U//FOUO) While attacks against pipelines and the oil and gas infrastructure are rare in the United States, they do occur with some frequency abroad. Islamic extremists clearly understand the economic significance of the gas and oil infrastructure, including pipelines, and see energy as a key center of gravity for Western nations. Intelligence reporting, public statements by terrorist leaders, and seized documents suggest terrorists have long seen the U.S. and global oil and gas industry as a high-value target and a prime means to disrupt U.S. and other Western economies.



(U) Trans-Alaskan Pipeline

(U//FOUO) In general, the U.S. pipeline system is resilient, and a major disruption to the supply would require multiple attacks. The U.S. system and its related infrastructure, however, are vulnerable to terrorist attacks because long stretches of unattended pipeline are difficult to protect. Nearly all pipelines in the continental United States are below ground—buried approximately two-and-a-half feet deep—but some portions are exposed, particularly in areas near highways, rail bridges, and inside tunnels. This is especially true in Alaska, where permafrost conditions and earthquakes require about half of the 800-mile Trans-Alaska Pipeline System to be above ground. The pipeline has the greatest amount of exposed pipe in the United States, making it a potential target for terrorists.

## (U) Most Likely Actors

(U//FOUO) Destruction of an oil and natural gas pipeline within the United States would clearly meet extremists' goals of causing economic and psychological damage to the United States. Al-Qa'ida remains the primary threat to the U.S. pipeline network; however, other terrorist groups also pose a threat.<sup>2,3</sup>



## (U) Al-Qa'ida

(U//FOUO) Al-Qa'ida continues to pose the most serious terrorist threat to U.S. and other Western interests, including pipelines and oil and gas infrastructure. In recent years, al-Qa'ida leaders have released multiple public statements inciting followers to attack U.S. oil interests overseas and in the Homeland. While al-Qa'ida leadership has not specifically targeted U.S. oil interests in these messages, the group has consistently viewed economic targets as a means to harm the United States and the West. Recent al-Qa'ida statements have maintained the group's overall message denouncing the West and targeting the United States and its allies.<sup>4</sup>

## (U) Recent Attacks by Al-Qa'ida and Affiliates

(U//FOUO) Al-Qa'ida and affiliated groups have historically targeted pipeline systems, and associated oil and natural gas facilities overseas, particularly throughout the Middle East. Many successful attacks have involved the use of small-arms fire, military ordnance improvised explosive devices (IEDs) and vehicle-borne improvised explosive devices (VBIEDs).

- (U) April 2008: Al-Qa'ida in Yemen claimed responsibility for a mortar attack against a complex in Yemen that housed American and Western oil executives. No injuries occurred.<sup>5,6</sup>



(U) April 2008: Al-Qa'ida attacks complex housing oil executives.

- (U) March 2008: An al-Qa'ida affiliate in Yemen—Jund al Yemen Brigades—claimed two attacks: a 29 March mortar attack against an unidentified Chinese oil company in Al-Khish'a and a 27 March bomb attack against a Total SA pipeline in the Sah Valley.<sup>7</sup>
- (U) November 2007: The Saudi Interior Ministry reported Saudi authorities arrested approximately 208 al-Qa'ida-linked suspects, including eight men who were allegedly planning to attack Saudi oil installations.<sup>8,9</sup>

(U//FOUO) Although there is no specific or credible intelligence indicating ongoing attack planning against critical domestic oil and natural gas facilities, al-Qa'ida has demonstrated both the capability and intent to attack energy infrastructure overseas and has expressed the intent to harm the U.S. economy. Al-Qa'ida could use attack methods proven overseas against oil and natural gas infrastructure in the Homeland.<sup>10</sup>

### (U) Other Transnational Extremists

(U//FOUO) Transnational extremist organizations with a presence in the United States include Lebanese Hizballah and the Palestinian Islamic Resistance (HAMAS). To date, their activity has been limited to fundraising; however, the potential remains that these groups could use their ties in the United States to bolster their operational and direct support capabilities should they decide to launch an attack in the Homeland. These groups currently lack the intent to target the U.S. pipeline system and the oil and natural gas infrastructure.<sup>11</sup>

### (U) Domestic Extremists

(U//FOUO) Domestic extremist groups typically are focused on single issues and include, but are not limited to, right-wing militias, animal and environmental activists, disgruntled employees, and lone individuals (lone wolves). Although domestic extremist groups have yet to demonstrate the intent or capability to launch attacks against the U.S. pipeline system, these groups have engaged in violence and criminal acts against oil and natural gas facilities.

(U//FOUO) Environmental extremists and other earth and climate agenda-oriented groups have disrupted international transportation systems by staging blockades and protest rallies at pipeline and other oil and natural gas infrastructure. Tactics have included banner hanging, tree spiking, tunneling, road blocking, mass mailings, stalking, human barricading, small-scale bombings, and incendiary attacks. Their aim is to gain attention to make a political statement, rather than hurt or kill people.<sup>12</sup> Many environmental extremists associate with other radical groups, such as Greenpeace, the People for the Ethical Treatment of Animals (PETA), and the Earth Liberation Front (ELF).

- (U) 1 April: A number of radical environmental groups initiated highly vocal “Fossil Fools Day” protests of the fossil fuels industry. The protests involved blocking traffic, banner hanging, covering the windows of the DNC Headquarters in Denver with green foam, and closing several ATMs throughout the San Francisco financial district by taping the ATMs with caution tape.

- (U) 18 February: The Earth First! environmental group conducted a blockade operation against the construction of a natural gas power plant in Florida.<sup>13</sup>



(U) 18 Feb: Earth First! blockade

### (U) Lone Individuals or Lone Wolves

(U//FOUO) Lone individuals or “lone wolf” extremists also present a threat to the pipeline industry. Because these individuals act independently, it is usually difficult to identify them or detect and disrupt their activity. Lone wolves usually have personal agendas or harbor grudges against specific single-issue targets.

- (U//FOUO) September 2007: A division safety manager of the Plains All American Pipeline, L.P. in Belen, New Mexico, reported seven bullet strikes in the junction line and associated valves. In this incident, it is difficult to determine if the intent was malicious target practice or intentional damage to breach the pipeline.<sup>14</sup>



### (U) Insiders

(U//FOUO) Industry insiders usually possess intimate knowledge of a company and may have access to controlled/critical areas. Terrorists or industry insiders could use this access and system knowledge to disrupt pipeline operations. Al-Qa'ida and associated terrorist organizations have expressed an interest in inserting their own operatives into employee positions to gain insider information and recruit specific individuals—based on their position, skills, and access to critical areas—in order to carry out acts of terrorism within the United States.<sup>15</sup>

- (U//FOUO) June 2007: The JFK bomb plot is perhaps the most recent incident of insider knowledge being used to threaten the pipeline sector. A former cargo worker at JFK used his knowledge of airport operations to assess airport security, identify the pipeline and fuel storage tanks as targets, and develop escape routes for a group, with no apparent links to al-Qa'ida, bent on carrying out a terrorist attack.<sup>16</sup>

## (U) Effect of Pipeline Attacks on Western Interests in Foreign Countries

(U//FOUO) Terrorist groups and organizations not necessarily desiring to attack the United States directly can still have an impact on the U.S. economy and pose a significant threat to U.S. and Western-owned and operated pipelines in foreign countries. For example, energy analysts estimate that attacks against oil pipelines in Iraq, Nigeria, Pakistan, and tanker ships in the Gulf of Aden have had a serious impact on global oil output, contributing to rising costs.

(U//FOUO) According to the U.S. Department of Energy, Energy Information Administration, the oil supply system continues to operate at or near capacity, and remains vulnerable to both actual and perceived supply disruptions. The combination of terrorist and criminal attacks, rising global demand, normal seasonal inventory patterns, slow gains in non-OPEC supply, and low levels of available surplus production capacity provides firm support for prices. Ongoing geopolitical concerns in a number of producing countries, including Mexico, Nigeria, Iraq, and Venezuela, have also contributed to crude oil price volatility.<sup>17</sup>

(U//FOUO) In particular, previous attacks and threats to attack U.S.- and Western-owned and operated pipelines in Mexico and the Niger Delta region have influenced U.S. fuel costs.

### (U) Mexico: Popular Revolutionary Army

(U//FOUO) In July and September 2007, Mexico's Popular Revolutionary Army (EPR), a Marxist-Leninist insurgent group, bombed natural gas and oil pipelines belonging to Mexico's state-owned Petroleos Mexicanos (PEMEX). The EPR claimed it carried out the attack to force the Mexican government to release imprisoned EPR members. The group has threatened continued attacks on Mexico's oil and gas infrastructure until their release

- (U//FOUO) Terrorists might strike directly at Mexican targets, given that Mexico provides a significant portion of U.S. oil imports and has other close economic ties with the United States. As a result, the Mexican administration took steps to protect Mexico and the United



(U) Mexican troops increase security at key installations after pipeline explosion in Queretaro, Mexico, on 10 July 2007.

States from international terrorists, such as deploying troops to protect critical infrastructure and tightening immigration procedures. The Oil and Gas Journal estimated that, as of 2007, Mexico was the sixth-largest oil producer in the world and tenth largest in terms of net exports.<sup>18,19</sup>

(U//FOUO) The EPR has not targeted any U.S.-owned pipelines or pipelines associated with Mexico's export of crude oil and natural gas to the United States. If the EPR were to change its targeting strategy, Mexico's crude oil and natural gas exports to the United States could be jeopardized.<sup>20</sup>

### (U) Nigeria: Movement for the Emancipation of the Niger Delta

(U//FOUO) U.S. oil companies and facilities in the oil rich southwest of Nigeria's Niger Delta remain under constant threat of attack from Nigeria's militant rebels and criminal groups, in particular, the rebel group Movement for the Emancipation of the Niger Delta (MEND). MEND attacks on foreign-owned oil facilities, pipelines, and company employees have reduced Nigeria's oil production by approximately 23 percent.<sup>21,22</sup> Throughout the year, MEND has entered into several ceasefire agreements with the Nigerian government that specifically references the cessation of attacks against pipelines. Thus far, these agreements have only been temporary. MEND's goal is to repeal current laws governing the distribution of oil wealth generated by the Niger Delta region.



(U//FOUO) MEND - Nigeria's largest militant rebel group - is an active terrorist group dedicated to armed struggle against the alleged exploitation and oppression of the people of the Niger Delta and the alleged degradation of the natural environment by foreign multinational corporations involved in the extraction of oil in the Niger delta.

(U//FOUO) Nigeria, the fifth largest foreign supplier of oil to the United States, exports approximately 40 percent of its oil to the United States, representing approximately 11 percent of U. S. oil imports.<sup>23</sup> Continued attacks on Nigeria's oil production infrastructure could significantly disrupt world oil markets and increase fuel costs to the U.S. transportation industry. Noteworthy attacks in 2008 include:

- (U) 26 May: MEND attacked a Royal Dutch Shell pipeline and engaged in a firefight with Army soldiers in the Niger Delta.<sup>24</sup>



- (U) 25 April: MEND conducted a string of IED attacks against pipelines in Nigeria's southern oil region.<sup>25</sup>
- (U) 14 April: The Nigerian government claimed MEND attacked two Nigerian Agip Oil company pump stations.<sup>26</sup>

### (U) Other Niger Delta Militant Groups



(U) Map of Niger Delta Region

(U//FOUO) More than 100 different Niger Delta militant groups thrive in this unstable area. The MEND, Niger Delta Peoples Volunteer Force, and the Niger Delta Vigilante Force are the predominant militant groups in the Niger Delta. However, militant groups in the region are deeply interlinked, making it difficult to establish the composition and structure of each group. Well-armed and organized groups attack foreign oil facilities, conduct criminal acts, intimidate security forces, and kidnap domestic and foreign oil workers. These activities are largely centered in, but not restricted to, the southern city of Port Harcourt and Niger Delta, which accounts for the majority of Nigeria's oil production activity.

- (U) January 2008: Militants in Port Harcourt, Nigeria, staged multiple attacks against oil company assets and personnel using IED and small-arms fire.

### (U) Colombia: Revolutionary Armed Forces of Colombia

(U) The Revolutionary Armed Forces of Colombia (FARC) is a large, independent,



FARC

self-sustaining Marxist-Leninist insurgent and drug-trafficking organization based in Colombia. (U//FOUO) The FARC is a major threat to the Colombian government. It occupies 40 percent of the nation's territory, mostly in the southeastern jungles and the plains at the base of the Andes Mountains. The FARC finances itself through ransom, extortion, and drug trafficking. The group extorts money from rural businesses, including agricultural, oil, and mining interests, for protection against attacks and kidnappings. The FARC has a history of attacking oil pipelines in Colombia by conducting small military operations against areas with light security.

- (U) March 2008: FARC rebels bombed an oil pipeline in Colombia using IEDs and small-arms fire.<sup>27</sup>

*(U//FOUO) The attacks on oil facilities in Muslim countries are often brought about by the presence of Westerners and Western companies on Muslim lands or the support that oil exports provide non-Muslim countries. Attacks may be less frequent in Western countries because there is no affront to the indigent population. Additionally, Western nations offer better industry security, better domestic security and police forces, and less accessible pipelines.*

## (U) Capabilities and Tactics

### (U) IED Attacks

(U//FOUO) IEDs have been the most prevalent weapon used in attacks on oil and gas facilities worldwide. Extremists often execute such attacks on gas and oil pipelines, and facilities and industry workers in Algeria, Colombia, India, Iraq, Indonesia, Myanmar (Burma), Nigeria, Sudan, Turkey, and Yemen, with the occasional, but rare, attack in Western nations.

- (U) July 2007: An IED partially detonated on top of a hardened access point to the NATO jet fuel pipeline outside of Italy's Dal Molin Airbase, Vicenza, Italy. The Anti Imperialist Team, a previously unknown leftist group in Italy, claimed responsibility for the attack.<sup>28</sup>
- (U) December 2006 and March 2007: Al-Qai'da in the Lands of the Islamic Maghreb detonated near-simultaneous attacks in Algeria employing sophisticated remotely-detonated explosive devices against U.S. and Russian vehicles carrying petrochemical industry workers.<sup>29,30</sup>

## (U) VBIED Attacks

(U//FOUO) Extremists often integrate small-arms attacks with VBIEDs for attacks against pipelines and oil facilities. Extremists used VBIEDs to attack oil facilities in Saudi Arabia in 2006 and Yemen in 2008. In both instances, security forces were able to thwart the attacks and reduce significant damage to the facilities and oil production.<sup>31</sup>

## (U) Standoff Weapons

(U//FOUO) Standoff weapons—such as anti-tank rockets, rocket-propelled grenades (RPG) or high-powered rifles—have been used to attack pipelines.

- (U) Chechen separatists continue to use mortars and RPGs in attacks on pipelines in Russia.<sup>32</sup>
- (U) The Free Aceh Movement in Indonesia has used small-arms ground fire and RPGs as a tactic against pipelines and related oil facilities in Indonesia.<sup>33</sup>
- (U//FOUO) In Iraq, according to multiple press reports, insurgents continue to use IEDs, boats, combined small-arms fire, and RPGs in their attacks on pipelines and fuel facilities.



(U) Pipeline fire in Iraq.

## (U) Cyber Attacks

(U//FOUO) At this time, the Transportation Security Administration's Office of Intelligence (TSA-OI) is not aware of any current terrorist threat to Supervisory Control and Data Acquisition (SCADA) systems at U.S. pipelines. SCADA networks, however, present a viable target. Large U.S. oil and gas pipeline systems rely heavily on SCADA networks.

(U//FOUO) SCADA, process, and distributed control systems are used widely in the chemical, electric power, natural gas and oil, telecommunications, transportation, and water sectors. Pipeline SCADA systems provide real-time information on pressure, rates of flow, and other operational data. Cyber exploitation of hardware or software vulnerabilities could impair the functioning of control systems, disrupt or degrade service, and possibly damage other infrastructure components.

(U//FOUO) According to a 2005 Department of Homeland Security (DHS) report<sup>34</sup>, al-Qa'ida and other Islamic extremist groups have shown a committed interest in acquiring the computer skills necessary for launching computer network operations, and alliances of convenience between outsider cyber experts and Islamic terrorist groups aiming to launch a cyber attack are plausible. The DHS report found:

- (U//FOUO) Most hackers have the ability to disrupt cyber countermeasures of critical infrastructures and breach SCADA systems. Their capability in particular depends on their technical skills and access to information systems' vulnerability information. These groups have shown an ability to produce virus and worm software, which could be used to overwhelm a SCADA system and affect its operations.
- (U//FOUO) Because their clandestine activities are unpredictable and difficult to detect, single individuals or small cells present a considerable challenge for the intelligence and law enforcement communities.
- (U//FOUO) The increasing connectivity and integration of SCADA systems have created multiple cyber points of entry that, if penetrated, would allow an attacker to extract proprietary or operational information, or manipulate system controls to disrupt or degrade performance.

## (U) Suspicious Incidents & Activity

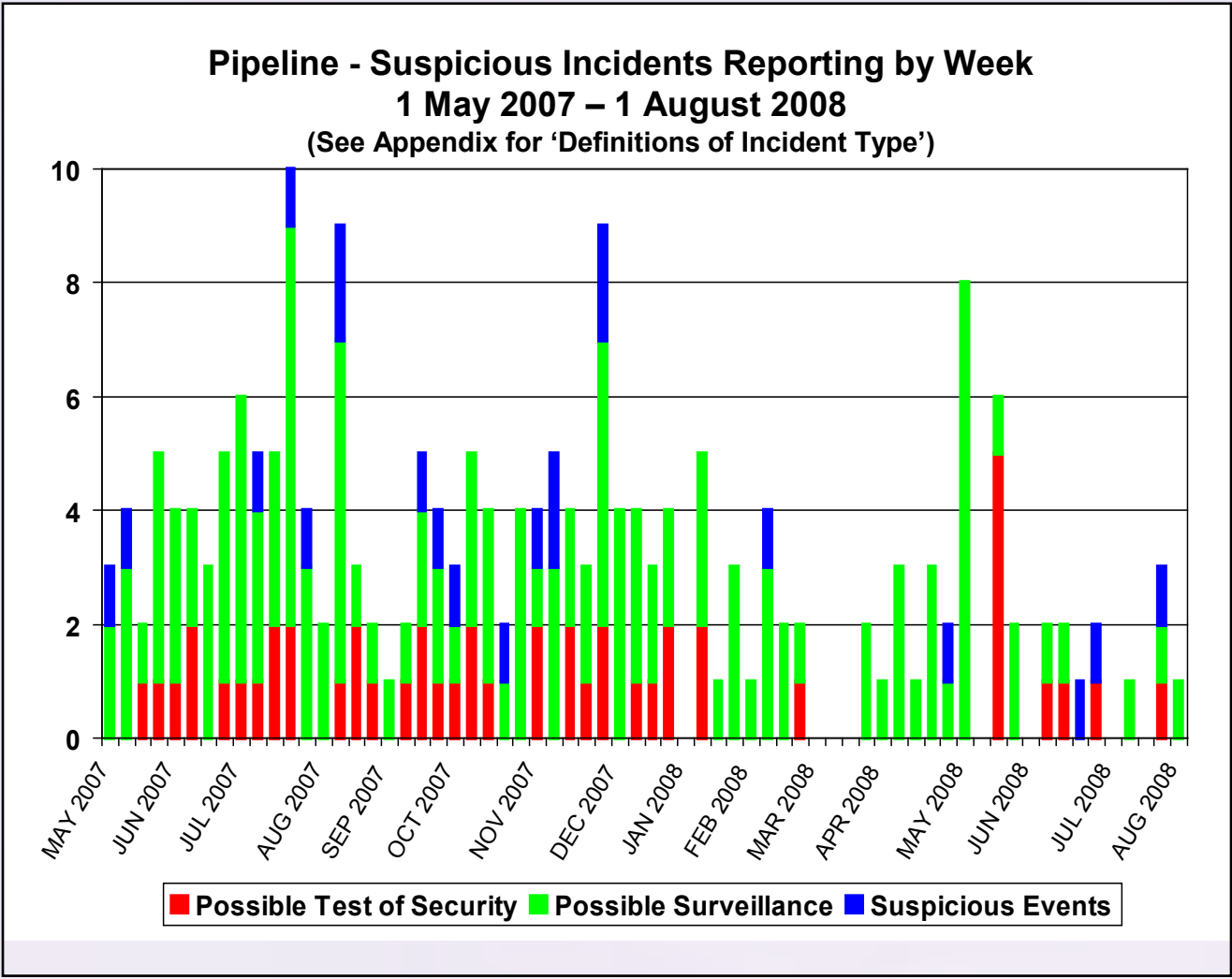
(U//FOUO) TSA-OI receives numerous reports of suspicious incidents involving pipeline and its related infrastructure (see chart next page). Of these incidents, reporting on photography, surveillance, and suspicious questions regarding pipeline and oil facilities are among those most frequently received. TSA-OI reviews of these incidents have revealed no definitive or direct ties to terrorism. However, reporting of suspicious activity can help law enforcement and security officials identify possible tests of security, surveillance activity, suspicious behavior, and criminal acts.

(U//FOUO) Suspicious incident reports received in 2008 include:

- (U//FOUO) 27 August: An unidentified male was observed photographing a U.S. refinery in Port Arthur, Texas.<sup>35</sup>



- (U//FOUO) 18 August: Three individuals were seen photographing a natural gas distribution point, located on top of Coal Mountain near Hurricane, West Virginia.<sup>36</sup>
- (U) 1 April: A pipe bomb exploded at a natural gas well site in San Juan County, New Mexico. Law enforcement officers believe that this incident was an isolated event, and do not believe that it was terrorism-related or part of a larger plot.<sup>37</sup>
- (U//FOUO) 23 March: A mobile security team saw an individual photographing an oil refinery and facilities in Roxana, Missouri. The individual fled in a vehicle when the team attempted to contact him.<sup>38</sup>



## (U) Conclusion

(U//FOUO) TSA-OI has no current or credible information that transnational terrorist groups or domestic extremists are planning to perpetrate an act of terrorism against the U.S. pipeline system, but long stretches of exposed, unattended pipeline make the system an attractive target. Although al-Qa'ida and its affiliates pose the primary threat to the U.S. pipeline system, environmentalist groups and domestic actors also pose a threat to this infrastructure.

(U//FOUO) While attacks in the United States are rare—only having been perpetrated by lone wolves and other non- nefarious actors with small arms—IEDs and VBIEDs have been very effective in attacks overseas on pipelines and associated critical infrastructure. Also of concern is the impact of attacks on U.S.- or Western-owned and operated pipelines in foreign countries and the effect these attacks could have on the U.S. economy and global oil market.

(U//FOUO) A terrorist attack on the U.S. pipeline system would likely result in widespread media attention and could have a regionally cascading impact on other transportation modes and critical infrastructure dependent on products carried through the pipeline system.

(U//FOUO) Suspicious incidents involving the pipeline infrastructure could be indicative of pre-operational planning for a future attack. A rise or sudden peak of interest in a pipeline facility could also be an indication of a bad actor's desire to draw a security response in order to ascertain potential vulnerabilities. The reporting of these incidents continues to aid in analysis of threats and trends to this sector.

*(U//FOUO) Prepared by the TSA Office of Intelligence, Transportation Intelligence & Analysis Division. For dissemination questions, contact TSA Production Management, [TSA-OI PM@tsa.dhs.gov](mailto:TSA-OI PM@tsa.dhs.gov).*

# APPENDIX

## (U) Definitions of Suspicious Incidents Terms (Chart pg. 9)

(U) The following terms, referenced in the chart (pg. 9) entitled, “Pipeline-Suspicious Incidents Reporting by Week,” are used to categorize types of suspicious activity related to transportation infrastructure—including the oil and gas industry:

### (U) Possible Test of Security:

- (U) The Misrepresentation – The use and/or misuse of false insignia, documents, or identification to misrepresent one’s affiliation in order to cover illicit activity
- (U) Theft/Loss/Diversion – Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents (classified or unclassified), which are proprietary to the facility)
- (U) Testing Security – Interactions with or challenges to installations, personnel, or systems that reveal physical, personnel, or cyber security capabilities
- (U) Cyber Attack – Compromising or attempting to compromise or disrupt an organization’s information technology infrastructure

### (U) Possible Surveillance:

- (U) Photography – Taking pictures/video of facility, infrastructure, personnel, or surrounding area
- (U) Observation – Showing unusual interest in a facility, infrastructure, and/or personnel (e.g., observing through binoculars, taking notes, drawing maps, or sketches)
- (U) Surveillance – Monitoring the activity of people, facilities, processes, and/or systems; Flyover – Suspected flight over a facility/infrastructure, including any type of flying vehicle (e.g., airplanes, helicopters, unmanned serial vehicles, hang gliders)
- (U) Eliciting information – Questioning personnel about facility, infrastructure, and/or personnel; This includes probing employees in person, on/off-site, over the phone, or via the Internet about particular structures, functions, and personnel procedures

### (U) Suspicious Event:

- (U) Sabotage/Tampering/Vandalism – Damaging, manipulating, or defacing part of a facility/infrastructure or protected site
- (U) Expressed or Implied Threat – Communicating a spoken or written threat to compromise a facility/infrastructure
- (U) Materials Acquisition/Storage – Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, timers); an unauthorized/unlicensed individual and/or group attempt to obtain precursor chemicals/agents or toxic materials and the rental of storage units for the purpose of storing or mixing chemicals
- (U) Acquisition of Expertise – Attempt to obtain training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling
- (U) Weapons Discovery – Discovery of weapons or explosives



# (U) ENDNOTES

- <sup>1</sup> (U) Joint FBI-DHS Bulletin; Intelligence Bulletin Number 242; 23 February 2007 “(U//FOUO) Jihadist Web Site Posting Renews Call to Attack Oil and Natural Gas Infrastructure;” (U//FOUO)
- <sup>2</sup> (U) FBI-Newark Counterterrorism Intelligence Bulletin, No. 9; 15 November 2006; “(U//FOUO) Potential Terrorist Pre-Operational Activity Targeting the U.S. Oil and Natural Gas Infrastructure;” (U//FOUO)
- <sup>3</sup> (U) Classified Document: National Intelligence Council, NIE 2007-02D; 1 July 2007; “(U) The Terrorist Threat To The U.S. Homeland”
- <sup>4</sup> (U) The Jamestown Foundation: www.jamestown.org; May 2006; “(U) Event Briefing: Saudi Arabian Oil Facilities: The Achilles Heel of the Western Economy;” (U)
- <sup>5</sup> (U) Oil & Gas Journal Exchange: orc.pennnet.com; 7 April 2008; accessed 22 May 2008; “(U) Al Qaeda Attacks in Yemen Latest to Target Oil;” (U)
- <sup>6</sup> (U) Reuters: Reuters.com; 7 April 2008; accessed 22 May 2008; “(U) Al Qaeda Says Behind Yemen Attack: Yemeni Official;” (U)
- <sup>7</sup> (U) Oil & Gas Journal Exchange: orc.pennnet.com; 7 April 2008; “(U) Al Qaeda Attacks in Yemen Latest to Target Oil;” (U)
- <sup>8</sup> (U) Open Source Center; GMP20080626837001; 26 June 2008; “(U) Saudi Interior Ministry Spokesman on Arrest of Militants in Saudi Arabia;” (U)
- <sup>9</sup> (U) The National Terror Alert; 26 June 2008; “(U) Saudi Arabia Disrupts Planned Terror Attacks on Oil Facilities-Arrest Hundreds;” (U)
- <sup>10</sup> (U) Classified document: DHS HSTA; 14 April 2008; “(U) Oil and Natural Gas Infrastructure: Louisiana and Texas”
- <sup>11</sup> (U) Classified Document: National Intelligence Council, NIE 2007-02D; 1 July 2007; “(U) The Terrorist Threat To The U.S. Homeland”
- <sup>12</sup> (U) Classified document: DHS HSTA; August 2007; “(U) Evaluating Known Threats and Anticipating Dangers”
- <sup>13</sup> (U) Environment News Service: ens- newswire.com; accessed 28 February 2008; “(U) Earth First! Blockades Florida Power Plan Construction;” (U)
- <sup>14</sup> (U) TSA: Transportation Security Operations Center, Executive Summary; TSA-10-3553-07; 29 September 2007; “(U//FOUO) Belen, NM: Suspicious Pipeline Activity;” (U//FOUO)
- <sup>15</sup> (U) Classified Document: National Intelligence Council, NIC NIE 2007-02D; 1 July 2007; “(U) The Terrorist Threat To The U.S. Homeland”
- <sup>16</sup> (U) Joint FBI-DHS Bulletin, Intelligence Bulletin No. 252; 4 June 2007; “(U//FOUO) Alleged Terror Plot against JFK Airport;” (U//FOUO)
- <sup>17</sup> (U) Department of Energy: Energy Information Administration; accessed; 6 May 2008; “(U) Short Term Energy Outlook;” (U)
- <sup>18</sup> (U) Department of Energy: Energy Information Administration; accessed; 28 August 2008; “(U) World Crude Oil Production, 1960-2007;” (U)
- <sup>19</sup> (U) Classified document: DHS; Homeland Security Office of Intelligence and Analysis Special Assessment; 20 February 2008; “(U//FOUO) Mexico: Building Counterterrorist Capabilities”
- <sup>20</sup> (U) TSA; Transportation Intelligence Gazette - TSA10 TG7-060; 23 July 2007; “(U//FOUO) Situational Awareness: Fuel Pipeline Attacks Result in Heightened Security in Mexico;” (U//FOUO)
- <sup>21</sup> (U) Mining Exploration; 20 April 2008; “(U) Shell Oil Mining Company Exploration in Nigeria, Supply Pipeline Explosive;” (U)
- <sup>22</sup> (U) Association for the Study of Peak Oil & Gas – Peak Oil Review, 5 May 2008, accessed 13 June 2008; (U)
- <sup>23</sup> (U) Department of State: Bureau of African Affairs; www.state.gov; June 2007; “(U) Background Note: Nigeria;” (U)
- <sup>24</sup> (U) AllAfrica.com; 27 May 2008; “(U) Nigeria: MEND Attacks Oil Facility;” (U)
- <sup>25</sup> (U) AfricaMasterweb.com; 24 July 2008; “(U) Chronology of Nigerian Militant’s Attacks;” (U)
- <sup>26</sup> (U) PunchontheWeb.com; 14 April 2008; “(U) Four Killed, Two Flow Stations Blown Up in Delta;” (U)
- <sup>27</sup> (U) Bloomberg.com; 6 March 2008; “(U) Colombia Pipeline Bombed by FARC after Ecuador Attack (Update 5);” (U)
- <sup>28</sup> (U) Italy Magazine; www.italymag.co.uk; 1 August 2007; “(U) Police Confirm Attempted Attack on NATO Fuel Pipeline;” (U)
- <sup>29</sup> (U) Open Source Center; GMP20061212214001; 122041Z DEC 06; “(U) GSPC Claims Responsibility for Algeria Bus Attack;” (U)

- <sup>30</sup> (U) Open Source Center; CEP20070304950015, 040959Z MAR 07; “(U) One Russian, Three Algerians Killed in Terror Attack in Algeria – Ministry;” (U)
- <sup>31</sup> (U) Open Source Center; GMP20060224541007; 24 February 2006; “(U) Saudi Arabia: 2 Car Bomb Attacks on Oil Refinery in Buqayq Foiled; Attackers Killed;” (U)
- <sup>32</sup> (U) Jamestown Foundation; Chechnya Weekly: Jamestown.org; 15 December 2004; accessed 13 June 2008; “(U) Chechen Rebels Are Trying to Damage Russia’s Oil-Gas Pipeline System;” (U)
- <sup>33</sup> (U) Publication: Schulze, Kirsten E;. ISBN: 1-932728-03-1; (U) “The Free Aceh Movement (GAM): Anatomy of a Separatist Organization;” (East-West Center, Hawaii, U.S. Publisher, 2004); (U)
- <sup>34</sup> (U) Classified document: DHS: Special Assessment; 12 December 2005; “(U//FOUO) Transnational Groups Ability to Compromise Supervisory Control and Data Acquisition (SCADA) Systems”
- <sup>35</sup> (U) DHS; NOC Patriot Report number 1670-08; 27 August 2008; “(U//FOUO) Suspicious Photography at a refinery in Texas;” (U//FOUO)
- <sup>36</sup> (U) DHS; NOC Patriot Report number 1621-08; 19 August 2008; “(U//FOUO) Suspicious Photography of a Natural Gas Meter/Regulation Facility in WV;” (U//FOUO)
- <sup>37</sup> (U) San Juan County Sheriff’s Office: www.sjco.com; 3 April 2008; accessed 4 September 2008; “News;” (U)
- <sup>38</sup> (U) DHS; NOC Patriot Report number 865811; 23 March 2008; “(U//FOUO) Suspicious Photography – Individual Observed Photographing Refinery;” (U//FOUO)