# Threat Assessment

## (U//FOUO) Chemical Facility Threat Assessment

8 June 2007

Homeland Security

Office of Intelligence and Analysis
Homeland Security

Threat Assessment

# (U//FOUO) Chemical Facility Threat Assessment

**8 June 2007**

*(U//FOUO) Prepared by the Homeland Infrastructure Threat and Risk Analysis Center.*

## (U) Scope

(U) The DHS Homeland Infrastructure Threat and Risk Analysis Center produced this threat assessment to support implementation of 6 Code of Federal Regulations Part 27, "Chemical Facility Anti-Terrorism Standards (CFATS)." This assessment describes the potential terrorist threat to the chemical and petroleum facilities regulated under CFATS and determined to be high risk by the Secretary of Homeland Security. It does not address facilities that may hold threshold quantities of the chemicals listed in CFATS that fall outside its scope, such as public water facilities or facilities regulated under the Maritime Transportation Security Act of 2002. Nor does it address the transportation of chemicals, which is regulated under other authorities. Potential terrorist tactics against such facilities—based on DHS' knowledge of terrorist intentions and capabilities—are included to aid industry security personnel in implementing security measures at their facilities.

***(U) 6 CFR Part 27: Chemical Facility Anti-Terrorism Standards***

***(U) Section 550 of P.L.109-295, of the 2007 Department of Homeland Security Appropriations Act authorizes DHS to establish risk-based (security) performance standards for high-risk chemical facilities. The Interim Final Rule issued by DHS in April 2007:***

- ***(U) Requires chemical facilities with threshold amounts of specified chemicals to provide information allowing DHS to make a determination whether each facility presents a high enough risk to be covered by the rule.***
- ***(U) Requires facilities determined by DHS to be covered by the regulation to conduct vulnerability assessments and develop site security plans to address identified vulnerabilities.***

## (U) Key Findings

***(U//FOUO) Intelligence reporting indicates al-Qa'ida, affiliated Sunni extremist groups, and other like-minded extremists continue to engage in operational planning with the intent to attack the Homeland.***

- ***(U//FOUO) None of the reporting to date has revealed any specific or credible threats targeting facilities in the nation's chemical sector.***

- ***(U//FOUO) DHS has received general information on threats to U.S. petroleum infrastructure—including refineries and petrochemical plants—but has seen no credible or specific intelligence indicating an imminent terrorist threat to the sector.***

***(U//FOUO) The tactics terrorists are most likely to use against the nation's chemical and petroleum infrastructure include aircraft as a weapon and vehicle-borne improvised explosive devices (VBIEDs). Many facilities also are vulnerable to cyber attacks against their supervisory control and data acquisition or business systems. Any of these tactics could include the use of insiders with access to and knowledge of sensitive facilities and systems.***

***(U//FOUO) Chemical and petroleum facilities are potentially attractive targets for terrorists.***

- ***(U//FOUO) An attack on a chemical sector facility containing large quantities of toxic industrial chemicals could cause fatalities, extensive injuries, and panic, and could generate heavy media attention.***

- ***(U//FOUO) Petroleum facilities appeal to al-Qa'ida and its affiliates because they symbolize what Usama Bin Ladin has referred to as "Western theft of the Muslim world's oil resources." Islamic extremists have attacked overseas petroleum facilities, especially in the Arabian Peninsula and Iraq.***

## (U) Threat Overview

(U) Al-Qa'ida and its network remain the greatest terrorist threat to the Homeland. This threat has evolved—from a small core directly led by al-Qa'ida—to encompass affiliated groups that are able to conduct attacks independently. Despite losses overseas and the emergence in the Homeland of a more formidable operating environment, al-Qa'ida has demonstrated resilience and kept its focus on attacking the Homeland. In addition, supporters of other, foreign-based Muslim terrorist and extremist groups—most notably Lebanese Hizballah and Palestinian HAMAS—are present in the Homeland. Some domestic groups also are a potential threat, albeit on a much smaller scale.

(U//FOUO) Use of conventional explosives—as opposed to chemical, biological, radiological, or nuclear weapons or materials—is the attack method al-Qa'ida is most likely to use against homeland targets. As the aviation plot in the United Kingdom revealed, however, attacking aircraft directly remains a key al-Qa'ida target, and it is likely that its leaders still see commandeering aircraft for 11 September 2001-style attacks as a viable method of achieving the group's objectives. The Intelligence Community has no specific information indicating al-Qa'ida is interested in attacking U.S. chemical facilities, but some types of homeland chemical infrastructure are potentially appealing targets. In addition, continuing terrorist attacks and plotting against petroleum infrastructure in the Middle East suggest that homeland oil and natural gas facilities also could be targets.

## (U) Terrorist Goals and Motivations

(U//FOUO) Al-Qa'ida's objectives in attacking the Homeland are to damage the economy, cause mass casualties and public panic, and to undermine confidence in the U.S. Government's ability to protect its citizens. Its ideology emphasizes that because the West—led by the United States—has declared war on Islam, it is not only acceptable but also imperative for Muslims to kill as many of their enemies—non-Muslim Westerners, especially Americans—as possible. The perception of Western governments as enemies determined to destroy Islam also justifies targeting symbols of Western nations and governments as well as symbols of economic supremacy. Bin Ladin has cited the oil industry specifically as a prominent target because of the alleged theft of Muslim oil by Western nations. Al-Qa'ida has conducted several attacks on oil infrastructure in Saudi Arabia and other Middle Eastern countries, but has not accorded high priority to attacking chemical facilities. The effects of such attacks, however, in some cases would comport with some of al-Qa'ida's objectives.

> ***(U) "Terrorism does not usually attempt to challenge government forces directly, but acts to change perceptions as to the effectiveness…of the government itself."***

## (U) Elements of a Major Terrorist Attack

(U) Analysis of terrorist attacks by al-Qa'ida and other international groups reveals that terrorists typically engage in a standard cycle for planning and execution of an attack (see table on next page).

| Activity | Comments |
|---|---|
| Broad Target Selection | — Strategic guidance provided by senior al-Qa'ida leaders, which may be provided through media statements.<br>— Individual cells may develop lists. |
| Intelligence Gathering and Surveillance | — Sophistication varies.<br>— Increasingly use the Internet for data collection.<br>— Activities may resemble suspicious incidents (elicitation, observation, photography) often reported by industry, but more sophisticated efforts may not be apparent.<br>— Represent potential opportunity to interdict cell/planners. |
| Specific Target Selection | — Political factors may mandate senior leadership approval.<br>— Affiliates may choose targets based on operational considerations (hardening of some targets may dissuade them). |
| Pre-Attack Surveillance and Planning | — Terrorists build attack plan, identify operators, and finalize data collection.<br>— Potential opportunity to identify/interdict.<br>— Activities may resemble suspicious incidents (elicitation, observation, photography) often reported by industry, but more sophisticated efforts may not be apparent. |
| Attack Rehearsal | — Used to test security or attack methodology.<br>— Difficult to discern from actual attack.<br>— Potential opportunity to identify/interdict. |
| Attack Execution | — Variety of factors influence tactics, such as nature of target and size and equipment of attacking force. |
| Escape and Exploitation | — Escape routes may be factored into attack planning.<br>— Attack may be videotaped or photographed for later exploitation.<br>— Not a factor for suicide attackers. |

**(U//FOUO) Table: Planning and Execution Elements of a Major Terrorist Attack.[*]**

## (U) Surveillance

(U) Surveillance is a substantial part of terrorist planning, occurring at several stages of the attack planning process. Terrorists may surveil facilities to collect intelligence, select targets, and to support operational planning. Because surveillance activity risks exposure, it is an opportunity for security personnel to identify and prevent an attack. Surveillance may not be readily detectable, however, because of its sophistication or the availability of other sources of information, such as the Internet to access maps and satellite imagery of potential targets and surrounding areas.

(U//FOUO) Chemical and petroleum companies regularly report activities resembling surveillance, such as photography, security breaches, and attempts to elicit information. DHS to date has not linked any reported suspicious incidents to preoperational surveillance or other terrorist activity. Suspicious incidents usually are attributable to a variety of motivations, including curiosity, criminal activity, employee disgruntlement, environmental activism, mischief, or vandalism. The number of suspicious incident reports has increased because of generally enhanced vigilance around most facilities and

[*] (U) Information in the "Activity" column is taken from U.S. Army Training and Doctrine Command, DCSINT Handbook No. 1: *A Military Guide to Terrorism in the Twenty-First Century,* Fort Leavenworth, Kansas, 15 August 2005.

the growth in public awareness of potential terrorist activity. Suspicious activities around chemical facilities do not differ markedly in their characteristics and frequency from those observed in most other critical infrastructure sectors. Most incidents are resolved by law enforcement and present no danger to U.S. infrastructure. Nevertheless, industry security officials should treat such incidents as potentially serious threats and report them to their local FBI Joint Terrorism Task Force and the DHS National Operations Center (NOC).

## (U) Chemical Infrastructure Threat Overview

(U//FOUO) Chemicals listed in 6 Code of Federal Regulations Part 27 are produced in both petroleum and chemical infrastructure facilities; Chemical Facility Anti-Terrorism Standards (CFATS) governs those facilities in each sector that hold the stipulated chemicals in threshold amounts.

(U//FOUO) Chemical facilities covered by CFATS are at risk from cyber or physical attacks, and theft or misuse of chemical products; any of which could be assisted by an insider. Terrorists could attack a chemical plant containing toxic industrial chemicals if their goal is to create a toxic chemical hazard imperiling lives or health, and create panic among the surrounding population. Terrorists also may target chemical facilities for theft of explosive or toxic materials for use in improvised weapons, or may try to obtain employment or recruit an employee to gain access to one or more of its products. Alternatively, they could attempt to present themselves as legitimate customers in order to purchase materials for illegitimate uses. DHS has no reporting to indicate a threat against the U.S. chemical sector from a cyber, insider, or physical attack.

## (U) Attractive but Difficult Targets

(U//FOUO) The most likely terrorist objective in an attack on a chemical facility would be to cause large numbers of casualties, create panic in the population, and to undermine confidence in the U.S. Government's ability to protect its citizens. Facilities near population centers are at greater risk in cases where the terrorist goal is to kill or injure large numbers of people and cause general panic.

***(U) Toxic Industrial Chemicals***

***(U) Numerous toxic industrial chemicals could be attractive terrorist targets because of their ability to cause casualties under the right circumstances. Chlorine is a common industrial chemical and has been used as an asphyxiate chemical warfare agent. It is one of many common industrial chemicals that could pose a downwind inhalation hazard in the event of a terrorist attack.***

***(U) Examples of toxic industrial chemicals that could be used as improvised chemical weapons include but are not limited to: ammonia, arsine, fluorine, hydrogen sulfide, hydrogen fluoride, hydrogen cyanide, hydrogen chloride, potassium cyanide, sulfuric acid, and some pesticides.***

(U//FOUO) Although an attack on a facility storing toxic industrial chemicals provides the potential to accomplish those goals, chemical facilities present challenges to prospective attackers. The lack of control over many key factors and the limitations in choice of weapons may help explain why terrorists have not yet attacked homeland chemical facilities. The success of an attack designed to cause extensive casualties from

the release of toxic industrial chemicals depends on factors frequently beyond terrorists' control or knowledge. These include:

- (U//FOUO) The specific chemical contents and quantities at any given time in targeted facilities.
- (U//FOUO) Meteorological conditions.
- (U//FOUO) Access to target materials with sufficient explosive power to achieve a toxic chemical release while not actually destroying the chemical itself.

(U//FOUO) Other factors also may discourage terrorists from attacking U.S. chemical facilities:

- (U//FOUO) On-site mitigation capabilities that could limit or contain the chemical release and overall damage caused by an attack.
- (U//FOUO) Off-site mitigation capabilities that could limit the impact of an attack on surrounding areas.
- (U//FOUO) Limited access to sufficient numbers and types of weapons capable of inflicting severe damage on a chemical facility.

***(U) Petroleum and Chemical Infrastructure***

***(U//FOUO) In evaluating threats to homeland infrastructure, the DHS Homeland Infrastructure Threat and Risk Analysis Center distinguishes between petroleum and chemical infrastructure to more precisely define the threat to each. Petroleum infrastructure consists of production facilities, refineries, pipelines, and other transportation modes, retail facilities, and terminal facilities. Chemical infrastructure consists of chemical and explosives manufacturing and storage facilities. Petrochemicals are produced at refineries and, therefore, are subject to attacks targeted at the petroleum infrastructure.***

***(U//FOUO) The threat to petroleum facilities and refineries is enhanced by the role of oil as a rallying point for Muslim ire against the West and the potential for attacks to inflict costly economic damage.***

***(U//FOUO) Chemical facilities have a less symbolic role. Terrorists may strike chemical facilities to trigger release of toxic industrial chemicals or to obtain access to chemicals for use as weapons or explosives.***

***(U//FOUO) Threats applying to either sector as a whole may not apply in full measure to individual facilities within them. In contrast, the threat to an individual chemical facility may be heightened because of its proximity to major petroleum infrastructure.***

## (U) Petroleum Infrastructure Threat Overview

(U//FOUO) Petroleum and petrochemical facilities covered by CFATS also are at risk from cyber or physical attack, and theft or misuse of chemical products, most of which could be assisted by an insider.

(U//FOUO) Al-Qa'ida leaders repeatedly have called for attacks on American oil interests overseas and oil infrastructure generally. In February 2007 a Saudi branch of al-Qa'ida called specifically for attacks on U.S. sources of oil throughout the world, emphasizing that targets should not be limited to the Middle East. The appeal identified Canada, Mexico, and Venezuela as U.S. oil suppliers. Attacks since 2001 on petroleum-related targets overseas have demonstrated the network's ability to strike all facets of the sector, including extraction, stabilization, refining, processing, distribution, and transportation of products.

(U//FOUO) Terrorist objectives in attacking petroleum infrastructure include striking blows against facilities symbolic of perceived U.S. "theft" of Muslim oil wealth and disrupting the supply of energy on which the United States depends. Attacks on petroleum facilities would pose a greater threat of causing an explosion than releasing toxic chemical substances, although in some cases a successful strike on a refinery could release toxic substances harmful to human health and the local environment.

***(U) Maritime Exemptions from Chemical Facility Anti-Terrorism Standards***

***(U) Many facilities that ship large volumes of chemicals of interest and are conducting vessel operations are governed by the Maritime Transportation Security Act of 2002 (MTSA) and are exempt from CFATS. Terrorist incidents at port facilities, however, may have security or other implications for nearby chemical facilities. For example, an attack on a port may inhibit transportation of materials to or from nearby chemical facilities, and an attack on a port or vessel in a port also may cause a release of hazardous materials into the surrounding area.***

***(U//FOUO) DHS has no credible intelligence to suggest operational planning for a terrorist attack on any MTSA-regulated facilities. Nonetheless, major port facilities and commercial shipping are symbols of and critical nodes for U.S. economic strength and, therefore, may be attractive terrorist targets. Furthermore, terrorists have attacked maritime targets abroad, such as the 2002 attack in which terrorists rammed a small boat with explosives into the French-flagged oil tanker M/V Limburg in the Gulf of Aden.***

***(U) Security managers of facilities near any waterway should be cognizant of the possibility that waterways could be used as an avenue of approach for attacking a facility. Examples include use of swimmers and small boats to access facilities surreptitiously.***

## (U) International Terrorist Groups

(U//FOUO) **Al-Qa'ida:** The most lethal of the Sunni jihadist groups, al-Qa'ida remains focused on directly attacking the Homeland and poses the most immediate and dangerous threat. Although hindered since 2001 by the death and capture of key operational planners and technical experts, and constrained by a host of security measures implemented by the United States and other countries, al-Qa'ida is a resilient and adaptive enemy with senior leaders fixated on striking the Homeland.

(U//FOUO) **Al-Qa'ida Affiliates or Sympathizers:** Many other groups inspired by al-Qa'ida are committed to global jihad and offer al-Qa'ida varying degrees of support. Al-Qa'ida has adopted a decentralized concept of operations whereby affiliated or sympathetic groups are encouraged to act on their own initiative consistent with the

organization's overarching goal of global jihad. The prospect that such groups may operate either in concert with or independent of al-Qa'ida to attack the Homeland is an issue of paramount concern.

***(U//FOUO) Traditional domestic extremists focus on specific issues or causes and select their targets based on certain practices or even associations with a targeted company. They often target corporations and their employees through harassment campaigns to compel them to change certain practices. In some cases, they have threatened to injure or kill individuals, but have yet to express an interest in producing mass casualties.***

(U//FOUO) **Homeland-based Supporters of International Extremists:** FBI investigations have revealed the presence of various Sunni extremists living in the United States, some of which have possible links to known terrorist groups, such as al-Qa'ida.[†] The focus of their activities centers primarily on fundraising, recruitment, and training, but some could be susceptible to al-Qa'ida exhortation to carry out terrorist operations in the Homeland, or they could decide to act independently. Lebanese Hizballah and Palestinian HAMAS both maintain an extensive presence in the United States, with operatives focused on providing support to their respective activities in the Middle East. These elaborate U.S. networks probably are capable of carrying out attacks within the Homeland.

# (U) Domestic Extremist Groups

## (U) Homegrown Islamic Extremists

(U//FOUO) Homegrown Islamic extremists are U.S. citizens or legal residents who become radicalized and seek ways to support the ideology and goals of radical Islamic groups. They reject the cultural values and beliefs shared by most Americans—including most American Muslims—and often sympathize with terrorist goals and in some cases feel driven to support or conduct terrorist actions.

(U//FOUO) Homegrown Islamic extremists do not necessarily confine their focus to the Homeland; some become involved in international terrorist organizations. Notable examples of homegrown Islamist extremists are John Walker Lindh[USPER], who left the United States to fight with the Taliban in Afghanistan, and Adam Gadahn[USPER], now an al-Qa'ida spokesperson.

## (U//FOUO) Traditional Domestic Extremists

(U//FOUO) Traditional domestic extremists pose a limited threat to homeland chemical and petroleum infrastructure. Most domestic, right-wing extremists focus their ire on government entities or racial minorities. Groups such as white supremacists, neo-Nazis, and the modern-day "militias" have not yet demonstrated particular interest in chemical or petroleum infrastructure.

[†] (U//FOUO) FBI listed 11 such groups with a presence in the Homeland.

(U//FOUO) Traditional domestic extremist groups, however—such as radical animal rights and environmental groups—have emerged as the most active domestic extremist threat. A primary objective of animal rights and environmental extremists is to attack corporations and other entities whose activities they perceive as contrary to their personal beliefs and ideological cause. Animal rights extremists oppose any experimentation on or euthanasia of animals; the environmental extremists target companies engaged in practices they believe degrade the environment. Animal rights extremists have targeted chemical and pharmaceutical companies, and environmental extremists opposed to oil drilling and some uses of petroleum products have targeted petroleum companies.

(U//FOUO) So-called "lone wolves"—such as individuals who have targeted the Trans-Alaska Pipeline and a California man who threatened to attack a refinery where he had worked—also pose threats to chemical and petroleum infrastructure.

## (U) Terrorist Attack Methods

(U//FOUO) Terrorists most likely would directly attack the chemical and petroleum infrastructure to destroy a facility, interrupt petroleum supplies, and release toxic industrial chemicals. Terrorists also could conduct cyber attacks on chemical or petroleum facilities to damage critical assets, disrupt or sabotage operations, or disrupt emergency response capabilities in coordination with a physical attack. Chemical sector facilities also face the possibility of theft, misuse, or diversion of sector products for use in an attack.

(U//FOUO) A wide range of terrorist tactics has been observed overseas, but terrorists within the Homeland would be limited by the choice of available weapons. Accordingly, DHS assesses that chemical and petroleum facilities within the Homeland are most at risk to physical attack by commandeered aircraft or explosives.

### (U) Aircraft as a Weapon

(U//FOUO) Commandeering and using an aircraft as a guided missile in attacks similar to those of 11 September 2001 remains a primary al-Qa'ida attack goal. Although terrorists may accord greater priority to using aircraft to attack high-profile iconic targets—such attacks against selected chemical and petroleum infrastructure could cause extensive physical damage, adversely affect the regional economic, and in some cases present serious public health and environmental effects.

### (U) Explosive Devices

(U//FOUO) VBIEDs have been the most effective means of terrorist attack in terms of numbers of casualties and property damage inflicted per incident. Al-Qa'ida has used this tactic repeatedly in attacking petroleum facilities overseas, and various enemy groups have used it frequently in Iraq against a variety of targets, to include petroleum facilities.

***(U) Materials Commonly Used by Terrorists in Explosive Devices***

***(U//FOUO) To produce any energetic, potentially explosive material, two components are needed: a fuel and an oxidizer. Oxidizers provide a source of oxygen to produce rapid combustion-like reaction when fuels are added to them. The FBI Explosives Unit identifies the materials listed below as those domestic and international terrorists most commonly use in constructing explosive devices.***

**Oxidizers**

Ammonium Perchlorate ($NH_4ClO_4$)
Sodium Chlorate ($NaClO_3$)
Calcium Hypochlorite ($Ca(OCl)_2$)
Ammonium Nitrate ($NH_4NO_3$)
Potassium Nitrate ($KNO_3$)
Hydrogen Peroxide ($H_2O_2$)
Barium Peroxide ($BaO_2$)
Potassium Permanganate ($KMnO_4$)
Lead Iodate ($Pb(IO_3)_2$

Lithium Chromate $Li_2CrO_4 \bullet {}_2H_2O$
Potassium Dichromate ($K_2Cr_2O_7$)

**Fuels: Hydrocarbons**

Gas
Diesel
Kerosene
Naphtha
Carbon Black
Charcoal

Sugar
Wax/Paraffin

Vaseline
Dextrin
Shellac
Rosin
Sawdust
Alcohol
Ethylene Glycol

**Fuels: Energetic Hydrocarbons**

Nitrobenzene (NB)
Nitromethane (NM)
Nitrocellulose (NC)

**Elemental "Hot Fuels"**

Powdered Metals
- Aluminum (Al)
- Magnesium (Mg)
- Magnalium (Mg/Al 50/50)
- Zirconium (Zr)
- Copper (Cu)

Phosphorous (P)
Sulfur (S)
Antimony Trisulfide ($Sb_2S_3$)

**Common Precursors**

Hydrogen Peroxide ($H_2O_2$)
Strong Acids
- Sulfuric ("Battery")($H2_SO_4$)
- Nitric ($HNO_3$)
- Hydrochloric ("Muriatic") (HCl)

Urea (fertilizer 46-0-0)
Methyl Ethyl Ketone (MEK)
Alcohol (Ethyl or Methyl)
Ethylene Glycol (antifreeze)
Glycerin(e) (Glycerol)
Hexamine (Camp Stove Tablets)
Citric Acid (Sour Salt)

(U//FOUO) To ensure enough explosive is used to produce a chemical release sufficient to cause mass casualties, DHS assesses that terrorists targeting fixed chemical or petroleum infrastructure would most likely rely on VBIEDs—either abandoning them at a target site for timed or remote detonation, or driving directly to a target and detonating them in a suicide mission. Manual delivery of an IED by an operative who emplaces it at the target or detonates it there in a suicide mission may be less effective against large, robust facilities because of the

***(U) The Internet has made information on developing explosive devices widely available and accessible. Although some of it is incorrect, there is enough accurate information for a person with no subject matter education or special knowledge to develop an effective explosive device.***

lack of explosive power, but could be used against remote, lightly protected infrastructure that is difficult to secure, such as pipelines.

— (U//FOUO) VBIEDs have the advantages of wide availability of bombmaking materials, concealment of large amounts of explosives in vehicles, and ease of maneuvering a VBIED to a target.

(U//FOUO) Terrorists planning to attack a chemical or petroleum facility would be expected to evaluate, among other things, what would be required to clear a path for a VBIED to reach one or more critical assets. Accessibility to the target determines how far away the blast occurs; blast effects decrease exponentially with distance from the target. Hardening potential targets against explosive attacks could limit access and increase the standoff distance between terrorists and facility assets; it could also prompt terrorists to select softer targets, increase the amount of explosives used to compensate for added standoff distance, employ multiple VBIEDs, or employ assault tactics to overcome obstacles prior to detonating the device.

— (U//FOUO) A VBIED attack could be facilitated by an insider providing support such as assisting with site access, distracting security, or identifying a path to the target.

(U//FOUO) A VBIED attack targeting a chemical storage vessel or other critical component may employ multiple vehicles accompanied by small arms fire to occupy or eliminate security personnel, clear a path between the facility perimeter and the primary target, and defeat or prevent implementation of defensive or mitigation measures. Al-Qa'ida operatives used similar tactics in attacks on oil installations in Saudi Arabia and Yemen in 2006.

## (U) Standoff Weapons

(U//FOUO) DHS has no information indicating terrorist intent to use standoff weapons such as artillery, rocket-propelled munitions, and guided missiles against Homeland chemical or petroleum infrastructure. On two occasions since 2001, however, FBI sting operations have thwarted the importation of surface-to-air missiles into the United States. Although these cases have not been linked to terrorism, they illustrate the potential for terrorist acquisition and use of such weapons.

(U//FOUO) Some large-caliber weapons are available within the Homeland, and concerns have been raised about their utility in attacking chemical storage vessels. Penetration of storage vessels by large-caliber projectiles does not guarantee an explosion because most flammable chemicals stored in bulk do not provide the fuel-air mixture best suited for causing an explosion. Even attacks on empty or nearly empty vessels that have not been purged—which provides more combustible conditions—are unlikely to produce catastrophic results. An incendiary round has a higher probability of causing a violent reaction of vapors, but still is not likely to cause an explosion when fired into a bulk

storage vessel. Leakage from a small rupture of a tank containing toxic industrial chemicals could be mitigated by facility and local safety and security plans.

## (U) Cyber Attack

(U//FOUO) Chemical and petroleum facilities use computers to monitor and process data such as flow, temperature, and pressure through supervisory control and data acquisition networks. Computers manage enterprise resource process systems and conduct automated measurement readings, while central or local control stations send signals to remote valves, opening and closing them to regulate flow or pressure or to seal them tight in an emergency. These capabilities improve the efficiency of the facility, but also expose the control systems to manipulation or disruption by malicious operatives, including terrorists.

(U//FOUO) Control systems are vulnerable to cyber attacks from inside and outside the control system network. The most elaborate boundary control program of firewalls, intrusion detection, and virus filtering will be of little help if an intruder or untrustworthy insider is able to gain physical access to servers, networks, or sensitive information.

(U//FOUO) Members of single-issue groups also may harness cyber capabilities to threaten and harass chemical and petroleum companies, although their goals are not likely to include physical destruction affecting the population and environment outside the targeted facility.

## (U) Purchase, Theft, and Misuse

(U//FOUO) Theft of chemicals from facilities or through diversion of chemical shipments—along with illicit purchases—in some cases could facilitate terrorist development of weapons and explosives. DHS has noted a small number of attempted purchases of chemicals that raised suspicion; none has been linked to terrorist activity and one case remains under investigation. Even legal purchases of certain materials in small quantities and from multiple sources can allow terrorists to accumulate sufficient quantities for use in building explosive devices.

(U//FOUO) Chemicals packaged in small amounts are more vulnerable to theft than those in other forms, such as tanks, vessels, or reactors. Several thefts of chlorine packaged in 150-lb cylinders or smaller have been reported; in contrast, an attempted theft of a one-ton cylinder of chlorine in California failed because the perpetrators were unable to operate facility equipment to move it.

(U//FOUO) Individuals seeking to obtain access to large quantities of certain chemicals may try to obtain commercial driver certifications allowing them to transport and potentially divert the chemicals. DHS is aware of a small number of instances in which individuals attempted to obtain credentials fraudulently that would allow them to drive trucks transporting hazardous materials. In one such instance, a student attending a truck driving school wanted to transport only chlorine, and in another instance, a student was

anxious to obtain a commercial drivers license and HAZMAT endorsement, but had no interest in learning important aspects of driving, such as backing up the truck.

# (U) Conclusion

(U//FOUO) DHS is not aware of any specific or credible threats to homeland chemical or petroleum sector facilities. Nonetheless, al-Qa'ida and affiliated Sunni extremist groups desire to attack the Homeland to damage the nation's economy, cause mass casualties, and undermine confidence in the U.S. Government's ability to protect its citizens. Homeland chemical and petroleum facilities are vulnerable to certain types of weapons and tactics, and for this reason remain attractive targets. DHS encourages owners and operators to remain vigilant and to report suspicious activities to the FBI and the DHS NOC.

### (U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operation Center (NOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the NOC can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@hq.dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

**(U) Tracked by:** HSEC-021200-01-05, HSEC-030000-01-05, TERR-060000-01-05, INFR-12000-01-05