

U. S. Department of Homeland Security
U. S. Coast Guard
Marine Safety Office Charleston
Marine Safety Information Bulletin

MSIB 28-04

June 29, 2004

Homeland Implications of Attacks on Energy Infrastructure Overseas

Recent terrorist attacks and incidents occurring overseas – perpetrated by al-Qaida or associated groups/individuals – continue to highlight terrorist interest in targeting energy related infrastructure. While we are unaware of any ongoing plans for similar, near-term attacks in the United States, al-Qaida’s demonstrated capability and intent to attack energy sector targets overseas suggests the potential that like attacks could occur inside the Homeland. Suspicious incident reports concerning possible surveillance of oil/gas refineries and infrastructure continue to emerge from throughout the Homeland and may, in some cases, be indicative of terrorist pre-operational activities. Al-Qaida views critical infrastructure targets – particularly businesses involving oil/gas – as attractive attack options because of their potentially significant economic, public health & safety, and psychological impacts.

On 29 May 2004, Islamic extremists likely associated with al-Qaida’s Saudi network, attacked the office of the Arab Petroleum Investments Corp and a residential compound, known as the Oasis Residential Compound, both located in the eastern Saudi city of Al Khobar. At least 22 people, including one American, were killed in this attack. An extremist leader named Abdul al-Aziz al-Muqrin claimed responsibility for the attack. On 1 May 2004, Islamic extremists killed seven Western workers at the offices of ABB Lummus Global, a contractor for the Exxon-Mobil/Yanbu Petroleum terminal, in Yanbu, Saudi Arabia.

On 24 April 2004, three closely-timed suicide boat attacks on Northern Arabian Gulf oil terminals in Iraq left two U.S. Navy sailors and one U.S. Coastguardsman dead, and five others injured. In the first incident, a U.S. Navy warship patrolling the gulf intercepted a boat as it approached the Khor al-Amaya oil terminal located approximately 100 miles from Iraq’s main oil port facility at Umm Qasr. As a U.S. boarding team approached the vessel it exploded, causing the fatalities and injuries. Twenty minutes later, two other boats approached the Basrah terminal, located twelve miles away from the first incident. As security forces intercepted the boats they also exploded, this time with no injuries. The Basrah terminal is Iraq’s primary export site for crude oil, the country’s primary source of revenue. A statement purportedly from Abu-Musab al-Zarqawi, a member of the Al-Qaida network, claimed responsibility for this attack. Indeed, Iraqi oil infrastructure has been a frequent target of extremist attacks.

SUSPICIOUS INCIDENTS IN THE U.S. HEIGHTEN CONCERNS

The Department of Homeland Security continues to receive suspicious incident reports involving oil and gas related infrastructure from the private sector, local and state authorities and concerned citizens from throughout the United States. While no identifiable trend or conclusive analysis has emerged from these incidents, activities characterized as possible pre-operational surveillance/information collection may have been conducted against energy sector facilities. Oftentimes individuals involved in suspicious photographing or videotaping of a facility would rapidly depart the scene before authorities could question and identify them. In some cases vehicle license plate registration checks reveal a mismatch between the license plate and the vehicle. Incidents reported also include possible security probes of facilities. The following represents a sample of reports received since August 2003:

Numerous incidents of possible pre-operational surveillance reported near a U.S. company's refinery facilities in several different states.

A northwestern U.S. company's field truck was broken into in a northwestern U.S. state, and a key ring with approximately fifty keys was stolen. The primary concern is the potential access to all of this company's facilities throughout the country. The national headquarters is taking action to change some locks locally.

A Facility Security Officer (FSO) witnessed an individual photographing a southern U.S. company's facilities, which had previously been the site of another incident of surveillance. Local law enforcement determined the vehicle involved was a rental. An employee at a southern U.S. oil terminal observed a suspicious female photographing pipelines. Two unknown males were observed inside a parked car nearby. When the facility Security Officer approached, the individuals departed.

An individual in a kayak was observed videotaping a northwestern U.S. company's refinery. The company's security personnel reported a suspicious encounter with a diver in the same general area last year.

Several incidents of suspicious activity over a three week period at a U.S. company's Southwestern U.S. fuel storage and distribution facility may be tests of security. Incidents included cutting the chain link and ramming an automobile through the fence. A gasoline tank trailer was reported stolen from a Northeastern U.S. company's lot. Local authorities are investigating.

A northeastern U.S. company reported an incident of possible surveillance of gas operations. Two males carrying a large video camera approached a gas facilities crew and identified themselves as being with an educational television network. When company personnel asked for identification, the two individuals refused and drove off. They were also seen videotaping a high school and a water tower in the area. Two males were observed taking pictures of a chemical plant and a bridge near a western U.S. port considered important to several refineries. The individuals claimed to be on vacation.

Multiple incidents were reported involving a northeastern port:

- Four foreign males approached a Coast Guard security gate and asked for directions. The men inquired about the facilities and what government agencies were present. When asked to leave, two male passengers, speaking in a foreign language, were pointing down the pier and writing down information.
- Soon after the above incident, one male and one female in a vehicle attempted to enter the same facility. They were denied permission to enter, and the security guard noticed two cameras with large 10-inch telescopic lenses.
- Additional earlier reporting indicates three individuals were observed videotaping the terminal.

SUGGESTED PROTECTIVE MEASURES

Additional domestic vigilance is recommended in response to the recent attacks overseas. Any suspicious incidents that may reflect pre-operational planning or surveillance of critical infrastructure should be reported immediately in order to identify developing trends and assist law enforcement officials conducting rapid investigative follow-up. In addition, to the implementation of facility security plans, may consider the use of the following recommended protective measures:

- Review perimeter security around critical facilities and consider expanding the buffer zone where warranted.
- Review your counter surveillance and intrusion detection methods and consider adding CCTV, motion detectors, intruder alarms, etc. as warranted.
- Check and verify credentials of all operators of official vehicles seeking entry into a facility.
- Consider equipping security staff with telescopic lens equipped digital cameras – this will enable them to photograph suspect vehicles and license plate numbers.
- Keep comprehensive records of all official identification cards, badges, decals, uniforms, and license plates distributed, document any anomalies, and cancel access for items that are lost or stolen.
- Practice accountability of all vehicles, including tracking vehicles that are in service, in repair status, or sent to salvage.
- Safeguard uniforms, patches, badges, ID cards, and other forms of official identification to protect against unauthorized access to facilities, including stripping all decommissioned vehicles slated for resale and/or salvage of all agency identifying markings and emergency warning devices.
- Check multiple forms of valid identification for each facility visitor.
- Verify the legitimate business needs of all approaching vehicles and personnel.
- Improve identification card technology to eliminate reuse or unauthorized duplication.
- Alert uniform store vendors of the need to establish and verify the identities of individuals seeking to purchase uniform articles.
- Ensure all personnel are provided a security briefing regarding present and emerging threats.
- Encourage personnel to be alert and immediately report any situation that appears to constitute a threat or suspicious activity.

If you have any questions regarding this matter please contact my representative, Mr. James Mahney at (843) 720-3276.

/s/

J. E. CAMERON
Commander, U. S. Coast Guard
Captain of the Port
Charleston, South Carolina