# New Reasons for Old Technology

CARRIE ELLIS, Editor

Imagine you're at sea aboard a chemical tanker. You see a rogue ship off in the distance. You realize that there may be a threat of hijacking, as you know these waters have been rife with pirates recently. Are you prepared? How have you protected others onboard, not to mention the potentially dangerous contents in the hull?

Along with this scenario, and other national terrorism scares like 9/11, came the advent of the Chemical Facilities Anti-Terrorism Standards (CFATS), which breed more responsibility, documentation, and stringent requirements for both the storage and transport of approximately 322 chemicals of interest. These chemicals range from the common—such as propane and ammonia—to the rare—like hexaethyl tetraphosphate.

The Department of Homeland Security (DHS) and other agencies claim that CFATS are necessary to eliminate easy targets of vast amounts of industrial chemicals, many of which are explosive, hazardous or otherwise sensitive. Furthermore, if you store, maintain, process or manage any of these chemicals in a certain quantity or concentration at any U.S. facility, it affects you directly, as opposed to the chemical manufacturer who may have provided them.

There are some exceptions to which facilities are affected, of course, including those owned or operated by the Department of Energy or the Department of Defense, facilities regulated under the Maritime Transportation Safety Act, public water systems as defined in the Safe Drinking Water Act, facilities subject to

regulation under the Nuclear Regulatory Commission and water treatment facilities as defined in the Water Pollution Control Act.

According to Ryan Loughin, director of petrochemical and energy solutions for the Advanced Integration division of ADT, “Safe and secure chemical storage and transport under DHS is based on the quantity of chemicals of interest at a facility, and the likelihood of a successful terrorist act at that facility. Facilities must either keep chemicals in quantities below those mandated or put in place a security plan that protects those chemicals from acts of terrorism.”

In 2006, Congress demanded that high-risk chemical facilities develop and implement security plans to guard themselves from potential terrorism. Then Congress authorized the DHS to administer appropriate regulations, and set fines of $25,000 per day, as well as force plant closures for those facilities out of compliance.

**What Does this Mean?**

Loughin says, “For the average facility, CFATS means going through a series of steps to first determine if the standards apply. If the facility is subject to CFATS, it can achieve secure chemical storage and transport by following the guidelines set by the DHS. The process starts with a Top Screen, then a Site Vulnerability Assessment (SVA), and finally the development and implementation of a Site Security Plan (SSP). The Top Screen analyzes the type, quantity, storage, manufacturing and handling of each chemical of interest. From there, the DHS assigns each facility with a preliminary tier between one and four, with one being the riskiest.

“Facilities are then required to perform an SVA, which takes a more in-depth look at existing security and vulnerabilities to come up with a final ranking based on the four tiers.” Depending on what tier a facility falls into, that facility “must include documentation of current security measures and address all 18 Risked-Based Performance Standards—which are established by the DHS—in its SSP. These standards include everything from perimeter security to record keeping. After the SSP has been developed, the DHS does a site inspection to make sure that all areas have been covered.”

**What To Do if Affected**

“CFATS is a performance-based standard, which means that the DHS does not specify the types of security measures to be used,” continues Loughin. “Instead, it looks at security to determine if a facility meets certain objectives. The mandate recognizes that facilities are very different, and no one-size-fits-all solution exists, and provides the flexibility to select solutions that work for particular situations. The DHS does recommend certain technologies for particular situations, but those are only recommendations.”

While many of the following technologies are not new, CFATS make them more necessary than ever for those who must deal with potential terrorist attacks, and

more advanced technologies are springing forth everyday to equip facilities with the requisite power to respond. Some solutions include:

- Perimeter barriers, intrusion detection systems or lighting.
- Surveillance or sensing systems.
- Inventory control equipment and documentation requirements.
- Identification or inspection terminals for vehicles or personnel.
- Professional security staffing.
- Cyber security.
- Appropriate monitoring equipment.
- Training.
- Record-keeping systems.

Since December of 2009, the DHS alerted upwards of 3,000 U.S. facilities that they must complete a Top Screen under CFATS. It is also estimated that more than 6,000 facilities must submit an SSP. Loughin's final advice for affected facilities is to "Work with knowledgeable security partners and consultants familiar with CFATS and DHS regulations." As the old adage goes, it is better to be safe than sorry.

*For more information, please visit the Department of Homeland Security via* www.dhs.gov *[1] or ADT via* www.adtbusiness.com *[2].*

**Source URL (retrieved on *10/23/2014 - 5:09am*):**
http://www.chem.info/articles/2010/07/new-reasons-old-technology?qt-recent_content=0

**Links:**
[1] http://www.dhs.gov/
[2] http://www.adtbusiness.com/