Understanding CFATS: What It Means to Your Business

Chemical Facility Anti-Terrorism Standards

John C. Fannin III, CPP, LEED^{AP}
Mark G. Wygonik, CPP

Advanced Integration

KCI PROTECTION TECHNOLOGIES

BACKGROUND

In 2006, the U.S. Congress mandated that "High Risk" chemical facilities develop and implement security plans to guard against the possibility of terrorism. Congress authorized the Department of Homeland Security to develop and administer the appropriate regulations. Congress established fines of $25,000 per day and closure of the facility as the penalties for any company found to be out of compliance. In 2008, DHS began the rollout of the regulation with the most significant and complicated portion of the implementation beginning now.

Introduction

The Chemical Facility Anti-Terrorism Standard (CFATS) is intended to establish a baseline level of security for facilities considered to pose high risk to the general population in the event of a terrorist attack. Many are under the mistaken impression that CFATS is a chemical facility regulation. It is, in fact, a regulation that covers facilities that use chemicals. This is a broader interpretation and more accurately defines the jurisdiction of the rule. CFATS defines security requirements for facilities that use, manufacture, store or handle specific quantities of approximately 322 chemicals that DHS has identified as being extremely dangerous. Affected industry sectors include chemical manufacturing, storage and distribution, energy and utilities, agriculture and food, paints and coatings, explosives, mining, electronics, plastics, and healthcare. These chemicals are called "Chemicals of Interest" (COI) and are listed in Appendix A of the regulation.

Appendix A of the regulation establishes a reporting threshold for the COIs. If a facility manufactures, uses, handles or stores any of these chemicals above the DHS set threshold, the facility must complete the CFATS Top Screen. The thresholds are described by a minimum quantity of the COI. Since many chemicals are used in solution, there is also a minimum concentration. If a facility has the COI in quantities below the threshold or in concentrations below the threshold, then the COI does not need to be reported through a Top Screen. The threshold is known as the Screening Threshold Quantity or STQ.

CFATS does not apply to all facilities. Facilities already under the jurisdiction of the Maritime Transportation Security Act (MTSA) are not covered, nor are Department of Defense owned or operated facilities or facilities regulated by the Nuclear Regulatory Commission. Other exempt sectors include public water systems and wastewater treatment facilities under U.S. EPA regulation.

DHS announced through the Federal Register, the promulgation of these regulations and the required compliance dates. The schedule began with the publication of the revised Appendix A on November 20, 2007. Facilities were given 60 days to complete their Top Screen.

Compliance with CFATS takes place in four stages:

I. Stage One: Top Screen

The purpose of the Top Screen is to evaluate all facilities housing quantities of potentially hazardous chemicals in an effort to develop a ranking on their relative risk. All facilities that used, manufactured, stored or handled any of the roughly 322 chemicals of interest in quantities above DHS-defined threshold limits must submit a CFATS Top Screen. The Top Screen gathers information on the type and quantity of chemicals used, stored, manufactured or handled by the facility. If the facility does not have these chemicals above the threshold, then the facility is not subject to CFATS. The Top Screen essentially evaluates the potential worst-case consequences if an incident were to take place at the facility.

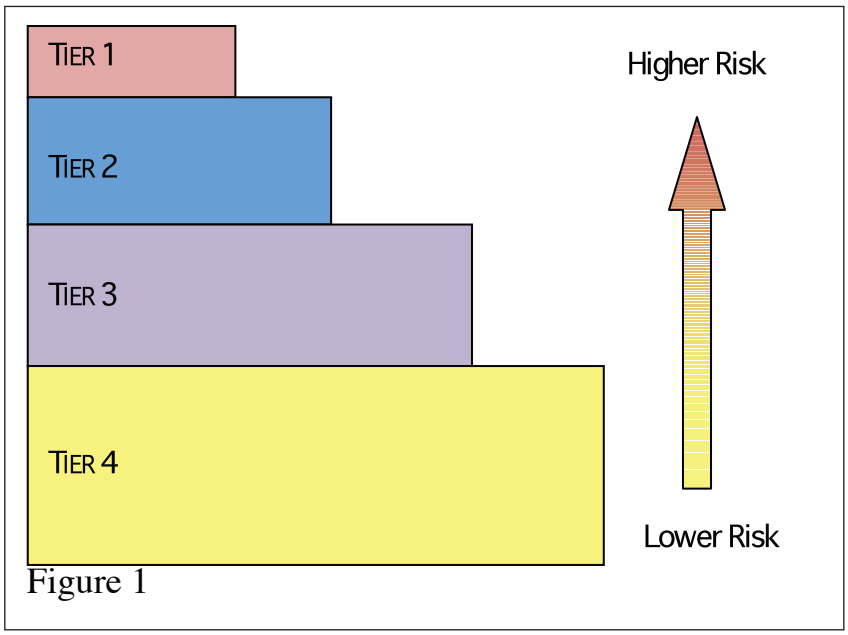


Figure 1

The Top Screen is completed online at a DHS secure website known as the Chemical Security Assessment Tool (CSAT). The facility answers questions about the quantity, location, phase and concentration of any of the COIs that they have had on-site during the past 60 days. In addition, COIs that have been identified as having a Release-based Security Issue undergo further evaluation. This evaluation uses U.S. EPA release tools to calculate the distance from the facility that might be impacted by a release of the COI.

There are two possible results from the Top Screen. DHS may determine that the worst-case consequences resulting from an incident at the facility do not reach the level classified as High Risk. These facilities receive a letter that informs them that they are not subject to CFATS at this time. (However, if the facility's inventory of chemicals changes, the facility must reevaluate its need to submit a revised Top Screen and do so as required.)

If DHS's analysis of the worst-scenario consequences do reach a level at which the facility is considered High Risk, the facility receives a letter communicating this status along with the following information:

- The names of the Chemicals of Interest that concern DHS.
- The Security Issues associated with these COIs (Security Issues are categorized as Release, Theft/Diversion, and Sabotage).
- The due date by which the facility must complete the next step in CFATS compliance (the submittal of a Security Vulnerability Assessment).
- The facility's preliminary Tier ranking (1, 2, 3 or 4; DHS has divided High-Risk facilities into 4 tiers of decreasing risk. Tier 1 is the highest risk, Tier 4 is the lowest of the high-risk rankings. See Figure 1).

II. Stage Two: Security Vulnerability Assessment (SVA)

If the purpose of the Top Screen is to divide facilities into risk rankings based on potential consequences, then the SVA seeks to determine the likelihood that the unwanted consequences can be prevented based on the security posture of the facility. Facilities that have received notification that they have been preliminarily "Tiered" must now complete a Security Vulnerability Assessment (SVA).

The SVA is completed online at a DHS CSAT website. The SVA requires each facility to identify critical assets associated with each COI listed in the Preliminary Tier Letter. The SVA website also requires that the facility inventory and describe their security equipment, their access control procedures and equipment, their inventory, shipping and receiving procedures. The facility is then instructed to evaluate the response and consequence of each critical asset /COI combination against a series of DHS-defined adversarial attacks.[i] These attack scenarios are based on the characteristics of the COI and the Security Issues[ii] listed in the facility's Preliminary Tier Letter. The facility is asked to consider an adversary's ability to conduct a prescribed attack against the listed asset/COI combinations and provide DHS with an informed judgment as to the level of success of the attack. The facility is also required to provide their value judgment on the effectiveness of emergency response programs.

This process may require as much as several hundred hours of effort to complete and may result in a final report that is several hundred pages long. It typically requires a team of personnel, each expert in different operational areas, to complete the SVA. It is critical that the subject facility provide consistent, accurate, precise and sound rationale to support its responses.

Facilities use the DHS CSAT website to submit their SVA online. DHS evaluates the results of the SVA and issues a Final Tier Letter to each facility. There are three possible results from the SVA:

1. DHS may determine that the consequences resulting from an incident at the facility do not reach the level classified as High Risk. These facilities receive a letter that informs them that they are not subject to CFATS at this time. (However, if the facility's inventory of chemicals changes, the facility must reevaluate its need to submit a revised Top Screen and do so as required.)

2. DHS's analysis confirms the facility's Preliminary Tier Ranking.

3. DHS's analysis of the SVA results in a change in Tier Ranking.

In either of these last two cases, the facility will receive a letter from DHS that confirms the facility's status as a High Risk facility. The facility is designated as a Covered Facility and subject to the next stage of the CFATS regulation. The notification letter received by the facility conveys the following information:

- The names of the Chemicals of Interest that concern DHS.
- The Security Issues associated with these COIs (Security Issues are categorized as Release, Theft/Diversion, and Sabotage).
- The due date by which the facility must complete the next step in CFATS compliance (based on 120 days for the development and submittal of a Site Security Plan).
- The facility's final Tier Ranking.

III. Stage Three: Site-Security Plan (SSP)

The Site-Security Plan ensures that covered facilities develop and implement a security plan appropriate for their relative risk. The plan must respond to the specific issues raised by DHS in its Final Tier Letter sent to each Covered Facility. The guide for developing the SSP is covered in a document called the "Risk-Based Performance Standards" (RBPS).

The RBPS is intended to provide facilities with flexibility in developing their SSP. Site-Security Plans must address 18 different parameters identified in the Risk-Based Performance Standards. Each covered facility must meet the performance requirements that DHS has established for each of these 18 security criteria. How the performance levels are met is at the discretion of the facility. Each Tier level (1, 2, 3 & 4) has a separate level of performance required. Therefore, although each facility must have a plan to restrict the facility's perimeter (RBPS 1), Tier 1 facilities, which represent the highest risk, have the most demanding performance requirements when compared with a Tier 4 facility.

Every covered facility must use the DHS online CSAT tool to describe their Site Security Plan. Much like a more in-depth SVA, the SSP online tool requires the facility to describe their security equipment, processes, procedures and plans. There are no attack scenarios involved, however, as the SSP follows the general outline of the RBPS. Facilities describe how they meet the requirements of each RBPS. Included in this process is a description of what the facility has in place now, what the facility is in the process of implementing (based on verifiable contracts and purchase orders) and what the facility is considering in the near future.

Once the SSP is complete, the facility submits it to DHS for review. DHS responds by issuing an analysis of the SSP that identifies gaps to be corrected, or it issues approval for the plan as described. The facility is informed of their deadline for complying with the next stage of CFATS.

RBPS 1 — Restrict Area Perimeter: The facility must provide effective measures for securing the perimeter to a level appropriate to the facility's Tier level. Perimeter security will likely include a combination of perimeter barriers, intrusion detection systems or other types of monitoring, lighting and protective forces.

RBPS 2 — Secure Site Assets: The facility must describe any additional measures it employs to secure and monitor restricted areas and critical targets within the facility. Critical targets may include not only locations where COIs are manufactured, stored or used, but also other critical assets, such as process controls, security and operations centers, and critical cyber assets. This RBPS is similar to RBPS 1, except that this performance standard focuses on the protection and monitoring of critical assets and COIs located within the perimeter of a Covered Facility. This RBPS must anticipate acts by insiders or insiders/outsiders teaming.

RBPS 3 — Screen and Control Access: The facility must describe the measures it employs to control access. Their response must focus on the identification, screening, and/or inspection of individuals and vehicles that enter and exit the facility. A variety of measures may be used for screening and access control, including procedures (identification and inspections of personnel and vehicles), control point measures (management of vehicular approach and entry) and parking security. Screening and access control seeks to prevent unauthorized access to the facility and to serve to deter and detect unauthorized introduction or removal of items that may cause chemical reactions, explosions or hazardous releases.

RBPS 4 — Deter, Detect and Delay: The facility must describe the measures it employs that provide for deterrence, detection and delay. DHS expects that Covered Facilities will utilize measures that will deter an adversary. In the event of an attack, DHS expects that the facility will employ measures that will detect the attack at the earliest point. DHS expects that the facility will use this early detection to employ other measures that will delay the point at which the attack is successful. Deterrence includes measures that prevent personnel and vehicles from penetrating the perimeter or gaining access to potentially critical targets, and includes such things as visible, professional and well-trained security personnel, well-maintained detection systems, barriers, barricades and hardened targets. Detection includes surveillance and sensing systems and countersurveillance techniques. Delay strategies are designed to provide sufficient time to allow for a response. Delay strategies include barriers and barricades, hardened targets and well-coordinated response planning.

RBPS 5 — Shipping, Receipt and Storage: The facility must describe the shipping, receipt and storage processes, procedures and technology that it employs to minimize the risk of theft, diversion, contamination or sabotage of any of its COIs. This includes inventory control measures, control of shipping containers, documentation requirements, authorizations or any other relevant measures.

RBPS 6 — Theft or Diversion: The facility must describe the processes, procedures and technologies that it employs to minimize the risk of theft or diversion. Like RBPS 5, this standard is focused on preventing the theft or diversion of potentially dangerous COIs.

RBPS 7 — Sabotage: The facility must describe the processes, procedures and technologies that it employs to minimize the risk of sabotage. In most cases, sabotage is considered an insider threat. In most cases, many of the measures previously d iscussed related to access control, monitoring, inventory control and perimeter security are applied to this standard.

RBPS 8 — Cyber: The facility must describe the processes, procedures and technologies that it employs to provide security for its cyber systems. These systems include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems. These are systems that are deployed throughout the operations of the facility which control sensitive processes, authorize and confirm access and enable general business operations. In describing its cyber security, the facility should expect to address its security policy, access control, personnel security, awareness and training, monitoring and incident response, disaster recovery and business continuity, system development and acquisition, configuration management, and audits.

RBPS 9 — Response: The facility must describe the processes, procedures and technologies that it employs to respond to security events. This addresses the response of appropriately trained personnel (either on-site facility personnel or off-site first responders) to a fire, aerial release or other loss of containment of a COI or similar incident. The facility must include descriptions of its notification and reporting procedures to on-site and off-site response personnel. It must also address the training it provides to response personnel and the exercises that it conducts with local emergency responders or mutual aid participants.

RBPS 10 — Monitoring: The facility must describe the processes, procedures and technologies that it employs to monitor the facility and to provide warning to on-site and off-site personnel. The facility should acknowledge any written procedures for the maintenance, testing, calibration and inspection of equipment as well as repairs and improvements to the system that increase reliability and improve response time.

RBPS 11 — Training: The facility must describe its policies and procedures for training related to security and response, exercises and drills. DHS expects that these training programs will include only personnel-specific exercises, drills and training, combining facility personnel, local law enforcement and first responders designed to improve first responder's understanding of the hazards and layout of the facility.

RBPS 12 — Personnel Surety: The facility must describe its policies and procedures for personnel surety. DHS expects that these policies and procedures will address background checks, verification of appropriate credentialing, procedures for approval or denial for work and access to the facility. Personnel surety is expected to include criminal history checks on a local and national level, verification of the candidate's legal authorization to work and screening against DHS's Terrorist Screening Database.

RBPS 13 — Elevated Threats: The facility must describe its policies and procedures for addressing the need for increased security during times of elevated threat as designated by DHS. The heightened security posture must explain how the measures taken by the facility increase the level of performance sought through the Risk-Based Performance Standards and how they reduce the likelihood of a successful attack.

RBPS 14 — Specific Threats, Vulnerabilities or Risks: The facility must describe its processes and procedures for responding to specific threats, vulnerabilities or risks, not originally identified, analyzed or evaluated in the original SVA. This describes how the facility will respond to threats specifically directed at it. The heightened security posture must explain how the measures taken by the facility increase the level of performance sought through the Risk-Based Performance Standards and how they reduce the likelihood of a successful attack.

RBPS 15 — Reporting of Significant Security Incidents: The facility must describe its policies and procedures for reporting security incidents through its internal management chain and, as appropriate, to external security and law enforcement entities. The policies should address the procedures used to determine the level of significance of a security event and the appropriate reporting mechanism.

RBPS 16 — Significant Security Incidents and Suspicious Activities: The facility must describe its policies and procedures for identifying, investigating, reporting and records retention of significant security incidents and suspicious activities in or near the facility. These procedures should address the identification of a qualifying event, the procedures for investigating the event, the manner and communication chain for reporting the event and a records retention policy covering the subject files.

RBPS 17 — Officials and Organization: The facility must identify at least one official, as well as the organization within the company, responsible for security and compliance with the RBPSs.

RBPS 18 — Records: The facility must describe its policies and procedures related to records retention of security-related material. This includes the creation, maintenance, protection, storage and disposal of these records and making these records available to DHS upon request.

IV. Stage Four: Implementation and Inspections

Once a facility's Site Security Plan has been approved, the facility has a set time within which it must implement its plan. DHS then begins a regime of on-site inspections to verify that the plan, as approved, has indeed been implemented. Implementation includes record keeping, training and exercises, as detailed in the RBPS requirements. DHS will inspect equipment, plans, processes, records and will observe operations. Noncompliance can result in fines of $25,000 per day and closure of the facility.

Facilities that fall into Tiers 1 or 2 must resubmit Top Screens every two years. Facilities falling into Tier 3 or 4 must resubmit Top Screens every three years. Any facility, whether currently subject to the CFATS requirements or not, must monitor their inventory of chemicals against the minimum thresholds established in Appendix A of the regulations. Any change that results in chemicals at or above the threshold quantities triggers the need for the facility to complete a CFATS Top Screen.

The future of CFATS

There is considerable speculation about the future of the CFATS program. The law granted DHS three years of authority to develop, promulgate and implement security measures for High-Risk chemical facilities. Legislation has been proposed to expand the jurisdiction of CFATS as well as to extend its life. It is possible that there will be some harmonization between the security requirements of the Maritime Transportation Security Act (MTSA) and CFATS given that so many chemical facilities operate under MTSA jurisdiction. There has been discussion of including municipal water and water-treatment facilities under CFATS as well as other permutations. But thus far, there has been no change.

Chemical Security Assessment Tool (CSAT)

The Chemical Security Assessment Tool is a secure website developed by DHS. It serves as the main platform for all CFATS compliance activities. CSAT provides the following functions:

1. It is the main registration tool for facilities that may be subject to the CFATS regulation.
2. It is the system used by facilities to input their Top Screen data and submit it to DHS for review.
3. It is the system used by facilities to input their Security Vulnerability Assessment data and submit it to DHS for review.
4. It is the system used by facilities to input their Site Security Plan information and submit it to DHS for review.
5. It is the system used by facilities to generate a new Top Screen based on changes to the types and volumes of chemicals associated with their operations or as required for periodic review by the CFATS regulation.
6. It provides covered facilities with additional information for completing various CFATS requirements.
7. It provides Covered Facilities with a tool for personnel surety (under development)

To access CSAT, a user must have successfully completed CVI training and have received a CVI certification number. The user must also be affiliated with a commercial entity that uses, handles, manufactures or ships chemicals. DHS provides the appropriate login information.

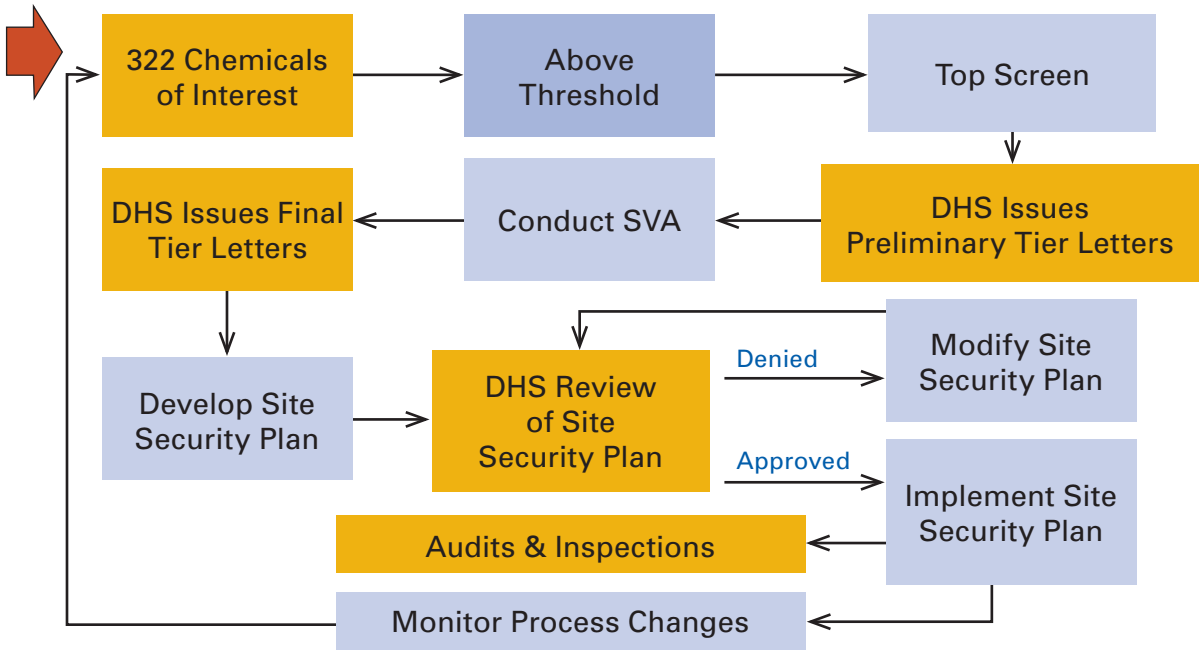
Relevant Statistics

DHS has indicated that approximately 36,000 facilities registered to conduct CFATS Top Screens. Of that number, approximately 6,419 were identified as subject to the Security Vulnerability Assessment requirement. These 6,419 were divided into the 4 risk tiers as follows:
182 Tier I [highest hazard]
681 Tier II
1,613 Tier III
3,943 Tier IV [lower hazard]
Not all facilities have completed their Top Screens. Facilities found to be out of compliance can face fines of up to $25,000 per day and the closing of their operations.

Chemical Terrorism Vulnerability Information (CVI)

Chemical Terrorism Vulnerability Information is a DHS program to provide security for information deemed to be sensitive but unclassified. It is specific to the CFATS program. CVI establishes a set of requirements for generating, handling, storing, distributing and destroying information generated during compliance with CFATS. It contains provisions that apply to private companies that are involved with CFATS as well as with local, state and federal personnel. DHS provides online training which results in individuals receiving CVI certification. Ongoing compliance with the regulation is subject to DHS audit.

An Overview of the CFATS Process



[i]CFATS Attack Scenarios

Aircraft Crash Attack

A1 Commercial aircraft (i.e., 737 size) crashes into facility in attempt to destroy large storage tanks of COI located in the tank farm area, separate from other process equipment.

A2 Adversary crashes commercial aircraft (i.e., 737 size) into facility in attempt to destroy large chemical processing area containing a variety of process equipment, including in-process inventories of COI.

Vehicle Borne Improved Explosive Device (VBIED)

V1 Adversary places VBIED outside of the facility perimeter, but located close enough (i.e., within 340 feet) for the vehicle bomb to destroy the COI storage tank or area considered the asset.

V2 Adversary cuts the facility back gate open during off hours (i.e., night or weekend operation) and drives the VBIED to a location at the end of the secondary containment closest to tank/area that is this asset.

V3 Adversary accesses the facility with a VBIED by entering the plant site behind a vehicle making an authorized entry or by crashing through a controlled access gate. The adversary drives the VBIED to the storage area or process unit that represents this asset and detonates the device there.

Maritime/Boat Borne IED Attack

B1 Adversary drives boat carrying IED on an off-site waterway that comes within 370 feet of the asset and explodes the boat at the closest approach point to the asset.

B2 Adversary drives boat carrying IED into an on-site waterway or channel that comes within 370 feet of the asset and explodes the boat at the closest approach point to the asset.

Assault Team Attack

AT1 Adversary team climbs or cuts the facility perimeter fence and places two explosive charges against the asset.

AT2 Adversary assault team attacks security assets at access control point and then moves through the plant on foot and places two explosive charges on this asset.

Standoff Attack

SO1 Adversary accesses the facility and fires the standoff weapon (i.e., light antitank weapon with shaped charge warhead) into the asset from a distance of 100 meters, initiating a release of a COI.

SO2 The facility is surrounded by a contiguous 7 ft. (in height) chain-link fence. Asset is within 100 meters of the facility perimeter and is easily visible from outside the fence. The adversary drives a van or delivery truck into the parking lot of an adjacent facility and uses the top of the vehicle as an elevated platform to launch a standoff weapon (i.e., light antitank weapon with shaped charge warhead) at the asset from a distance of 100 to 200 meters.

Theft

T1 Adversary team enters the facility and steals largest portable container on-site, leaving the facility in a vehicle without immediate awareness by facility staff (i.e., no immediate law enforcement notification and pursuit).

T2 Adversary team enters the facility in a vehicle, obtains one or more portable containers of the theft COI, and successfully leaves the facility in the vehicle without being detected.

T3 Adversary enters the facility on foot and steals one or more man-portable containers, moving them to transport vehicles outside of the facility.

Sabotage

SA1 Adversary (insider or outsider) accesses placarded amount of COI that is designated for shipment and contaminates largest placarded amount/shipment from the facility in a manner that will result in an explosion or toxic release at some point after shipped from the facility.

SA2 Adversary (insider or outsider) accesses placarded amount of COI designated for shipment and contaminates one or more placarded amounts (selecting shipments that are easily contaminated). The containers are then shipped from the facility, and the contamination results in an explosion or toxic release at some point after shipped from the facility.

Diversion

D1 Adversary is allowed to register as a customer to purchase COI and have it shipped to the adversary's chosen location.

D2 Adversary is allowed to file a false order for an existing customer that results in shipping the COI to a location that is not controlled by the approved customer.

D3 Adversary is allowed to accept shipment of or pick up an order with COI that is intended for an approved customer.

[ii]**Security Issues:** The CFATS SVA process looks at the characteristics of the Chemical of Interest and the manner in which that chemical may be used as a weapon. Some chemicals may be stolen and used to make an Improvised Explosive Device (IED). Some chemicals may be stolen and used to create a chemical weapon or some other form of a mass-effect weapon. In other cases, an adversary may create a catastrophic release of the chemical of interest, resulting in an explosion, a fire or the discharge of a cloud of toxic fumes that may harm facility personnel and local inhabitants. DHS describes these events as "Security Issues" and they include: Release — Toxic; Release — Flammable; Release — Explosive; Theft/Diversion; Sabotage.

About the Authors

John C. Fannin III, CPP, LEED^{AP} serves as president of KCI Protection Technologies. With a distinguished career spanning more than 30 years, he has provided risk analysis, industrial security, and fire protection engineering services to the chemical industry since 1979. He has been involved with some of the earliest risk assessment activities for the chemical and other infrastructure sectors, predating CFATS regulations. John is experienced in VAMCAP®, Carver, Sandia RAM and other credible vulnerability assessment methodologies and analysis processes.

Mark G. Wygonik, CPP has extensive experience in engineering, analysis, project management and policy development in the areas of risk management, security vulnerability assessment, threat assessment, and consequence analysis. He has worked in critical infrastructure areas, such as transportation, manufacturing, and food and agriculture. As risk analysis division chief, Wygonik heads the CFATS initiative at KCI Protection Technologies.

About ADT Security and Its Advanced Integration℠ Division

ADT's Advanced Integration Division (formerly SST) has a Petro-Chem & Energy Solutions team dedicated to serving the Petrochemical industry. This team has petrochemical **security experience pre-dating 9/11, MTSA and CFATS** and has the knowledge help deliver solutions in support of these regulations. In addition, each team member is certified and can help customers develop and establish total security management plans for perimeter detection systems, video surveillance and access control. ADT Advanced Integration provides the following services: system consultation, project management and coordination, system installation and commissioning, general construction, system training, and maintenance and service. Plans are implemented with a practical approach to help configure an integrated security solution that is efficient and cost-effective.

ADT Security Services, Inc. ("ADT") is a unit of Tyco International and part of ADT Worldwide, the world's largest electronic security provider. In North America, ADT provides electronic security services to nearly 5 million commercial, government and residential customers. ADT's total security solutions include intrusion, fire protection, video systems, access control, critical condition monitoring, home health services, electronic article surveillance, radio frequency identification (RFID) and integrated systems. ADT's government and commercial customers include a majority of the nation's *Fortune* 500 companies, all U.S. federal courthouses and over 70 mid-to-large airports. Headquartered in Boca Raton, Florida, ADT has more than 24,000 employees at approximately 240 locations in the U.S. and Canada. ADT's services go beyond the installation of security systems. ADT is **SAFETY Act certified and designated** for Electronic Security Services from the U.S. Department of Homeland Security.

For more information about petrochemical and energy security solutions from ADT Advanced Integration, please call 1-888-446-7781, or visit www.ADTbusiness.com/petrochem

About KCI Protection Technologies

KCI Protection Technologies LLC (KCI-PT) provides innovative technical, scientific and management solutions in security, fire protection, risk analysis, life safety and emergency management. With a professional staff of engineers, scientists, analysts and assessors, KCI-PT delivers products and services related to the protection of people, property, information and mission against preventable losses. KCI-PT products and services include strategic advisory services, technical assistance, consultation, engineering design, planning, conformity assessment, software and information resources, program development and specialized training.

KCI-PT provides comprehensive compliance services regarding the United States Department of Homeland Security, Chemical Facility Anti-Terrorism Standards (CFATS). KCI-PT professionals have been involved with some of the earliest risk assessment activities for chemical and other infrastructure sectors. Our multidisciplined approach to chemical process safety, industrial security, fire protection and life safety enables us to provide clients with unique engineering, consultation and analysis services throughout the CFATS compliance process. KCI-PT offers an easy-to-use CVI Security Guide™ to assist facilities with Chemical-Terrorism Vulnerability Information (CVI) security. For more information, please call 302-479-7000, or visit www.kci-pt.com

VR 01192009

L7916-00

ADT Advanced Integration

KCI PROTECTION TECHNOLOGIES