Ten Tips for Completing a Site Security Plan

Introduction

The Chemical Facility Anti-Terrorism Standards (CFATS) program requires covered facilities to submit a Site Security Plan (SSP) using the Department of Homeland Security (DHS) Chemical Security Assessment Tool (CSAT) website. The SSP is a crucial step in any facility's compliance program. It communicates to DHS how the facility provides security within the CFATS framework, and it lays the foundation for a regulatory agreement between DHS and the facility. Given the importance of the SSP, covered facilities should address a number of factors while they complete this step in the CFATS regulation. This paper presents 10 specific areas for consideration.

Many facilities are covered by CFATS and considered "High Risk" by DHS. To date, many of these facilities should have already received notice from DHS of their final Tier rankings (1, 2, 3 or 4), but others have yet to be notified. Final notice starts the next stage in the CFATS compliance process, the submission of the SSP. In this notice, DHS confirms a facility's Tier ranking, identifies the Chemicals of Interest (COI) that the facility must address with its security program, and specifies the relevant Security Issues. Facilities now should be actively engaged in completing the groundwork necessary for submitting their SSP.

What follows are 10 suggestions for those individual facilities that are working on their SSPs. These suggestions are offered for consideration. They will not apply to every facility, and for those facilities for which they do apply, they will not apply uniformly. In particular, those individuals who hold the role of "Authorizer" for the purposes of the CFATS program should review these suggestions to determine the extent to which they may inform their specific CFATS program.

Ten Tips for the CFATS Site Security Plan

1). Develop Your Plan Before You Begin the SSP

The facility staff responsible for completing the SSP should plan and document the facility security program *before* beginning to input information into the DHS SSP website. The CFATS SSP uses a series of questions posed by DHS. These questions are designed to obtain information regarding how a covered facility addresses security, based on 18 Risk Based Performance Standards (RBPS). DHS reviews a facility's answers and makes a determination if the security measures in place (or planned) are sufficient.

Since Congress mandated that DHS use a performance-based approach to chemical facility security rather than a prescriptive approach, there is no "right answer" to these DHS questions. DHS has provided guidance and examples of what it considers appropriate, but the agency cannot foresee every set of circumstances. This leaves facilities with latitude on how to approach such things as access control, detection, delay and deterrence.

EXAMPLE: RBPS1 — Restrict Area Perimeter

Facilities initially may think the appropriate action is the installation of a fence line around the entire facility. But before making this investment, facilities should take into consideration their Tier level, their COIs and the types of security issues they must defend against. The higher the Tier ranking, the higher the performance expectations for nearly all of the RBPSs, but this is also factored against the type of security issues. Facilities having only theft and diversion issues must find ways to control access to the COIs, while facilities with release issues must defend against armed adversaries and other attack scenarios such as vehicle bombs. Facilities with both of these security issues must defend against both.

Restricting the area perimeter might be achieved with other vehicle barrier strategies such as berms, bollards or landscaping in conjunction with surveillance and intrusion detection systems. Strategies appropriate for large facilities in remote or rural settings may differ significantly from more compact and urban facilities. The trade-offs between and integration of various security technologies and operational procedures combine to form a facility's security strategy or security program.

Where to Begin

Covered facilities should start their security planning based on what they know. During the Security Vulnerability Assessment (SVA) process, facilities identified critical assets, which can be thought of as targets of attack. For each facility, DHS identified the COIs, the security issues and the threat scenarios. DHS also identified the Tier level, which, when linked to the RBPS, defines the level of security DHS deems appropriate for the facility. Starting with this information, facilities can identify the combination of security technology and policy and procedures that, when combined and integrated, provide a security strategy it believes appropriate for the requirements of CFATS. With this overall strategy, the facility now can begin to craft its answers for the online SSP questionnaire. The end result of submitting answers to the SSP is that each facility essentially negotiates its individual regulated program with DHS.

2). Know What Your Tier Level Means

Of the many facilities that DHS classifies as High Risk, not all are created equal. High-risk facilities have been further categorized by DHS into four Tiers, with Tier 1 representing facilities with the highest associated risk and diminishing risk associated with Tiers 2, 3 and 4. The Tier level establishes the level of performance that the facility will need to provide for the 18 Risk Based Performance Standards (RBPS). Facilities should understand the effects of their Tier level on the RBPS. More than half of the RBPSs have differing levels of performance requirements linked to a facility's Tier.

EXAMPLE: RBPS1 Restrict Area Perimeter

A Tier 1 facility must provide "an extremely vigorous, high-integrity system to secure the perimeter that severely restricts or delays any attempts by unauthorized persons to gain access to the facility." For the same RBPS, Restrict Area Perimeter, a Tier 4 facility must provide "a system to secure the perimeter that reduces the possibility of access to the facility by unauthorized persons." It is clear that the expectation on the part of the Tier 1 facility is that the system used to restrict the area perimeter will have a high likelihood of success of keeping unauthorized personnel from gaining access while the Tier 4 approach is expected to reduce the likelihood of success.

Given that a facility also will know its security issues (release vs. theft/diversion), the facility will know what DHS prescribed attack the perimeter is expected to face and should plan its approach to perimeter security accordingly. The Tier 1 with release issues will need to consider such things as standoff distances, crash-rated barriers and line-of-sight between critical assets (targets of attack) and attack positions inside and outside the perimeter.

3). Understand the Ramifications of "Release" Security Issues and "Theft & Diversion" Security Issues

"Release" security issues focus on the consequences that may be generated by virtue of the covered facility's proximity to population centers and other critical assets. If such a facility is attacked, on-site COIs may be released onto the facility and into the surrounding community. The release may take the form of a toxic vapor enveloping a population center, an explosion with its related on- and off-site consequences, or a fire with its related on- and off-site consequences. The facility itself essentially serves as the weapon.

The Implications of "Release" Security Issues

Covered facilities must provide security strategies that detect, deter, delay and respond to armed attacks. DHS provides facilities descriptions of the attack scenarios and adversarial capabilities, including trained and armed commando-style teams along with various types of improvised explosive attacks. Some of these scenarios leave the facility with little likelihood of interdicting an attack; therefore, a facility needs to plan appropriate responses. With other scenarios, the facility must present security strategies that have a likelihood of successfully detecting, deterring and delaying an attack, providing adequate time for an appropriate response that will interdict the attack. Facilities should be in a position to show how their security strategies provide adequate time from the point of detecting an attack to the point that the planned response is effective.

Release security issues have a significant impact on the security strategies of a covered facility due to the armed attack nature of the threat. Facilities facing these issues likely will need to consider layered deterrence and coordinated on- and off-site response planning. The violent nature of the threat readily identifies an ongoing attack; however, it also places serious demands on a facility's security strategy.

The Implications of "Theft & Diversion" Security Issues

Theft and diversion security issues rely more on undetected access either to the COIs or to management systems that control the movement of the COIs. Theft and diversion focuses on a facility as a source of a COI that will be taken by an adversary using stealth and used as a weapon at a later time and at a different location. Typical targets are COIs that may be used as weapons of mass effect, may be converted into weapons of mass effect or which may be fabricated into explosive devices.

Facilities faced with these security issues are required to implement security strategies which limit and control who has access to the COIs and how the COIs are moved. Facilities will need to develop and document procedures and policies that control how the subject COIs are ordered, stored, handled and shipped. It likely will be a combination of security technology and procedures that a facility will implement to exercise the level of control over its COIs required by DHS. Facilities will likely need to demonstrate that they can keep COIs from unauthorized personnel, and in the case of an attempt to acquire such material, the facility will detect the adversarial actions with sufficient time to respond appropriately. Training, written procedure and cyber security will be strong contributors to security strategies applied against theft and diversion threats. Facilities should be prepared to illustrate the adequacy of their security strategies designed to control access to COIs and the provisions for deterring or detecting unauthorized access to and movement of COIs.

4). Include All of Your Critical Assets in Your Plan

Facilities that completed their Security Vulnerability Assessment (SVA) provided DHS with a list of critical assets. The list of critical assets that is reported in the SSP stage of implementation should match what was previously reported. Any changes that may have eliminated an asset from consideration as critical should be documented and available for the DHS site inspections that are to follow. Facilities should be prepared to justify these changes.

DHS also has indicated that on-site assets not considered critical based on the SVA definition may be found to be critical based on the ability of an adversary to use the assets as weapons against a critical asset.

EXAMPLE:

A tank used to store small quantities of vehicle fuel located in close enough proximity to a critical asset that the fuel tank's destruction can be used to initiate damage of the critical asset. In this case, the fuel tank substitutes for an adversary-provided improvised explosive device. The ramification of this position is that assets not previously provided consideration in the security strategy planning may be pulled into the SSP during a DHS site visit. Facilities might consider conducting a review of assets and attack scenarios with this in mind, to anticipate the possibility that DHS may designate previously excluded assets as critical. Facilities with higher Tier rankings and with "Release" security issues may be more likely than others to be subject to this interpretation.

Facilities also should be sure to address security strategies for control systems and cyber assets that are used to control processes and manage business operations. The potential for an adversary to use cyber assets to create a release, divert a COI, impersonate a legitimate customer or shut down a portion of a security asset all constitute threats that need to be addressed by a facility's security strategy. It is not just RBPS 8, Cyber Security, that is at issue. It is also the physical security of cyber assets that should be addressed. It is essential that a facility control access to computer hardware and other cyber assets. It also is essential that monitoring and control systems be protected from physical harm and be designed with an appropriate level of redundancies.

5). Apply the Concepts of Control, Deter, Detect & Delay

Most aspects of the security plan sought by DHS for covered facilities can be achieved by applying four simple principles: Control, Deter, Detect and Delay. When taken in a broad context, these principles will aid a facility in developing its CFATS security strategy.

Control. This is the ability of a facility to manage its activities and assets. Control requires that a facility have policies, procedures and technologies in place that establish rights, authorities and responsibilities and to provide monitoring and feedback. Control applies to nearly every aspect of security, from designating who has access and what they have access to, to determining how access is granted and monitoring how that access is used. Control applies to information as well as access to physical space and assets. Control also requires that a facility maintain a reporting and management structure that supports the allocation of authority and responsibility.

Deter. This is the perception on the part of the adversary that the effort required to mount a successful attack is greater than that required for an alternative target. A successful deterrence program leads to reluctance on the part of the adversary to mount an attack or drives the adversary to select an alternative facility. Deterrence can be enhanced by providing separate layers of security, such as requiring personnel to pass through several control points to gain access to a COI. The more protection that exists between an adversary and a targeted asset, the lower the likelihood that the adversarial attack will succeed.

Detect. This is the ability for the facility to identify the fact that it is under attack. The sooner the attack is detected, the sooner an appropriate response can be mounted. Detection is equally important to "Release" security issues as it is for "Theft & Diversion." Detection is the first step in response. Facilities should consider how soon their security program will alert personnel to the breach of a perimeter or to an attempt to gain unauthorized access to a COI or other critical asset. The sooner an attack, including "Theft & Diversion," is recognized, the sooner an appropriate response can be initiated.

Delay. This is the ability of a facility's security program to keep an adversarial attack from succeeding long enough for an appropriate response plan to be deployed. Delay may be a function of several layers of security impacting an attack, such as combinations of barriers, doors and fences. Delay may also be generated by limiting vehicle movement and reducing visibility. Facilities should consider how their security strategies build in delay for its type of security issues. "Theft & Diversion" delay may be attained through the use of multiple gates with authorizations required, crash-rated fencing or other techniques that allow the facility to recognize the attack and respond.

These principles of Control, Deter, Detect and Delay are integrated into the overall Risk Based Performance Standards. RBPS 4, Deter, Detect, Delay highlights these principles, but they are essentially the basis for the ability of the security strategy to perform.

6). Record Your Answers & Rationale

Every facility should record the answers that are submitted via the SSP. In addition to the answers, **facilities should also record the rationale for the answers. Creating this record will prepare the facility for the DHS site inspections that are part of the CFATS program.** Facilities might consider generating the answers along with the rationale in a separate document to allow management and legal review before submission to DHS through the SSP. Establishing a record of how the SSP data was developed will be of value when discussing options and compliance with DHS. In the case where DHS challenges the ability of the SSP to meet the requirements of the RBPS, the facility will have already generated its justification documents.

7). Consider Using Industry Standards & Best Practices

As facilities make decisions on the technologies, policies and procedures they adopt and implement to comply with CFATS, a wide range of value judgments will be required. Although the RBPS provides guidance, as does the DHS CFATS website, facilities may be faced with decisions that have significant cost and operational consequences. Facilities will likely work to comply with CFATS in the most economical manner. In these situations, facilities might consider looking to industry standards and best practices that closely reflect their specific circumstances. Organizations that have issued standards and guidelines related to security plans and technology include groups such as ASTM, CCPS, ASME, NFPA, ASIS, ACC and others. Standards and guidelines have been issued on topics ranging from security fencing, gates, lighting, mass notification and access control. The use of such standards and guidelines allows the covered facility to leverage the work and consensus of other groups, providing the facility with justification for its position.

8). Generate a List of Security Procedures

Every covered facility will be faced with deploying procedures used by its personnel to enact its security measures. Facilities will need to have written copies of these procedures distributed to those individuals responsible for carrying them out. Each facility should maintain these procedures, train their personnel and periodically review and revise them. Facilities might consider procedures for such things as: visitor inspection, delivery vehicle inspection, periodic inspection of area perimeter, security equipment maintenance, security equipment calibration, personnel background checks, emergency response, incident investigation and others. Procedures should be reviewed whenever there is a material change to the operation of the facility. In addition, facilities should establish a policy for the periodic review of all procedures.

Maintaining these procedures likely will be an important aspect of ongoing security measures at covered facilities. It is likely that DHS inspectors will seek out copies of procedures or question on-site personnel on the use of certain procedures.

9). Generate a List of Responsible Personnel

When developing its security strategy, each facility will serve its interests and prepare for completing the SSP by developing a management plan for security and communication. This is of particular importance in response planning. RBPS 17, Officials and Organization, sets the requirement for covered facilities to designate a chain of command. Doing so in writing not only will aid in meeting this RBPS requirement, it will help personnel understand their responsibilities for security, incident communication and record keeping.

10). Seek Help with Your Plan

Many facilities are required to participate in this regulatory program. Some of these facilities will share some of the same questions and challenges. There is no need for a facility to face these challenges alone in the development of its compliance program. As each Tier submits their SSP, the body of knowledge for this regulation grows. DHS further refines its guidance information and updates its Frequently Asked Questions page. Sources of help include DHS itself, which offers compliance assistance visits that may provide a facility with some on-site guidance. There are seminars and planning information provided by industry trade groups and user groups, and of course, there is a wide variety of consultants and physical security integrators.

Don't Forget CVI

Though not covered in detail in this article, the Chemical-Terrorism Vulnerability Information (CVI) program establishes requirements for the protection of sensitive but unclassified information. The information submitted as part of the SSP will be covered by CVI. Facilities should understand how the CVI security program works. Facilities should have appropriately trained staff and certified individuals who have a valid "Need-to-Know" to handle these materials in accordance with the CVI program. Mishandling CVI information can be grounds for noncompliance just as easily as a weak area perimeter or lack of inventory controls. Be sure to comply with CVI while you are complying with other aspects of CFATS.

Summary

The Chemical Facility Anti-Terrorism Standard represents a new area of regulatory activity for the federal government. As a result of 9/11 and the increased awareness of the consequences of terrorism, Congress has directed DHS to address security issues involving high-risk chemical facilities. As Congress continues to review other risks attributed to facilities that use, store or handle chemicals, it is likely that the CFATS model will be applied to other industry sectors. The facilities currently working on implementation of CFATS have the challenge of being the first through such a program. DHS itself is new to the security regulations arena, and is developing critical mass and a body of experienced personnel. But this process will experience starts and stops along with unanticipated changes in direction. Covered facilities should proceed with caution and with the understanding that what is a requirement today may shift tomorrow.

About ADT Security and Its Advanced Integration™ Division

ADT's Advanced Integration Division has a Petro-Chem & Energy Solutions group dedicated to serving the petrochemical industry. This group has petrochemical security experience predating 9/11, MTSA and CFATS and has the knowledge to help deliver solutions in support of these regulations. In addition, each group member is a certified CVI (Chemical-Terrorism Vulnerability Information) Authorized User and can help companies 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

VR 05012010

L8176-00

ADT Advanced Integration