CFATS: Surviving the Site Security Plan

Tips for Inspection & Resubmission

Updated July 2012

Introduction

As the Department of Homeland Security (DHS) moves forward with the Chemical Facility Anti-Terrorism Standards (CFATS), the program continues to evolve — and grow. It is essential that the regulated community follows its evolution closely. This white paper is intended not only to describe the ongoing CFATS compliance process (which is a combination of technical, procedural, and personnel security) as currently known, but also to provide insight regarding how to prepare for a CFATS Authorization Inspection (AI). The recommendations below are relevant to Site Security Plans (SSPs) for all tier levels and should be considered for a facility's initial SSP submission and/or any required SSP resubmission.

The SSP Review Process

DHS initially scores the submitted SSP with a computer-generated program that analyzes the "radio button" answers. The SSP is then reviewed by various DHS subject matter experts (SMEs) to reconcile "Other" box answers and any additional documents or information uploaded with the SSP. (Some examples of possible supporting documentation are provided in the "Painting a Picture" section of this white paper.) From a scoring perspective, positive consideration is also provided to "Planned Measures." For example, if the facility's SSP indicated that it "planned" to implement security measures in the future, such as the addition of intrusion detection, cameras, or even policies and procedures, DHS will credit the facility for the forthcoming security measures and verify their authenticity during the inspection process.

Of course, as a performance-based regulation, DHS can only prescribe the security outcome — such as a secure perimeter — but cannot prescribe how, specifically, a facility must achieve the outcome for its assigned risk tier (i.e., Tier 1 — Tier 4) and applicable Chemical of Interest (COI) Security Issues (i.e., Release, Theft/Diversion, or Sabotage).

Know Your Regulatory Audience

The officials responsible for approving (or denying) a facility's submitted SSP have not seen (and likely will never see) the facility. In other words, the "boots-on-the-ground" inspectors observe, report, assess, and validate but do not make the actual approval/denial decision regarding the adequacy of the SSP. Therefore, it is essential that facilities plan their SSP submission accordingly and endeavor to "paint a picture" of their security posture and environment.

Painting a Picture

Rather than simply answering "Yes" for a question, answer "Other" and take the opportunity to give an expanded written answer. The information in the "Other" boxes should describe, in detail, the facility's security posture, including physical security as well as specific procedures and policies. Take credit for measures already in place, even if those measures do not fit perfectly within the scope of the question, and use the "Other" box to provide sufficient detail.

Supporting documents, diagrams, maps, and graphics also help "paint a picture." These may include descriptions of policies/procedures, safety guidelines, satellite imagery, or drawings depicting the location of COIs within the facility. This information can be uploaded directly into the Chemical Security Assessment Tool (CSAT) SSP in virtually any file format. Painting the picture also means identifying the type and extent of facility assets for the purposes of Risk Based Performance Standards (RBPS) 2 (Secure Site Assets).

Completing Planned Measures and Proposed Measures for each RBPS is another way to provide a more comprehensive portrait of your security measures and how they may meet the RBPS Guidance. Unlike Planned Measures that DHS will use for compliance purposes, Proposed Measures are intended to spur further discussion with DHS but will not be used as part of DHS's SSP scoring process.

Submission Strategies: All RBPSs Are Not Created Equal

When developing a strategy for your SSP submission, consider designating CFATS "assets" under RBPS 2. How, where, and to what extent a facility designates CFATS assets is an essential part of a facility's protection philosophy. Study portions of the RBPS guidance referring to protection at the facility level versus the asset level for different Security Issues and COIs. For instance, a Release COI may be treated and protected differently than a Theft/Diversion COI. The proper protection philosophy for facility assets can fundamentally affect your SSP submission and your CFATS compliance approach.

Try to leverage enterprise resources. Corporate-level approaches may be appropriate for several RBPSs. For example, the security measures utilized for safeguarding cyber/IT resources may rely heavily on preexisting corporate-level procedures that apply at the facility level and can be used to help satisfy RBPS 8. This may also be true for many of the latter RBPSs (11-18). The idea here is to utilize all available measures, policies, and procedures.

Ensure questions are answered consistently across the RBPSs. A number of questions repeat themselves, specifically in RBPS 1 (Restrict Area Perimeter), RBPS 2 (Secure Site Assets), and RBPS 4 (Deter, Detect, and Delay). For instance, if you indicate "Yes" for "Fixed view" CCTV cameras in RBPS 1, ensure "Yes" is selected for "Fixed view" CCTV cameras in RBPS 4.

Ensure your technology-based security measures complement each other and accurately portray the layers of protection that are fundamentally required to satisfy each RBPS for physical security. As applicable, ensure your security force, CCTV system, intrusion detection system, and monitoring and response mechanisms create a seamless execution of the security picture you "paint" in the SSP.

Pre-Authorization Inspections

In early 2010, DHS added an additional step in the SSP approval process occurring after a site submitted its initial SSP through the CSAT: the Pre-Authorization Inspection (PAI). DHS determined that this step was necessary to gain additional information from facilities that did not provide adequate support or detail for SSP answers in their original submittal. Following the PAI, DHS allowed facilities to make SSP changes by unlocking the CSAT for "Technical Edits," enabling additional information and detail to be added to the original SSP. However, at this time, it is unknown whether DHS will continue the PAI process, which DHS appears to have suspended as of the date of this writing.

Authorization Inspections (AIs)

The AI represents an opportunity for DHS to physically visit a facility, meet with facility personnel, and verify the security measures and procedures described in the facility's preliminarily approved SSP submission. At least historically, the DHS AI team typically consists of four to six inspectors who spend multiple days on-site.

In preparation for the AI, all employees and personnel who may come in contact with the inspection team should be briefed on appropriate procedures and expectations. For example, the inspectors expect to complete the same safety or facility orientation requirements that any other site visitor must complete prior to site access. Obviously, brief all relevant security/reception personnel accordingly. Ensure the facility is prepared and organized to include the ability to react quickly to DHS requests for information and documents. As you prepare for the AI, remember that certain information is subject to ongoing Chemical-Terrorism Vulnerability Information (CVI) safeguarding requirements. Copies of all CFATS correspondence and submissions — such as the Final Tier Notification Letter and the SSP, among other things — should be readily available. Some facilities may want to conduct a full-scale rehearsal, to the extent that it is possible.

Authorization Inspection Delays

In December 2011, an internal DHS memorandum evaluating the current state of the CFATS program was leaked to the news media. The memorandum identified a number of significant shortfalls and challenges that have stifled the program, including an inefficient SSP review process and inadequate and inconsistent internal training capabilities — and ultimately resulted in several congressional hearings. As a result, DHS suspended conducting AIs in order to review the process and ensure its inspectors received appropriate and consistent training. The inspector training course began in Spring 2012 and is expected to conclude in Summer 2012 — after which DHS has indicated it will resume the AI process.

Conclusion

The CFATS compliance process can be burdensome and may, at times, seem overwhelming. Try to be as proactive as possible in preparing for upcoming CFATS submissions, including developing a submission timeline, allocating the appropriate personnel and resources, as well as collecting all relevant policies and procedures. As the CFATS program continues to march on, the AIs are DHS's "close targets." Understanding the process and DHS's expectations is essential to navigate this new and uncharted area of regulatory compliance.

For more information about petrochemical and energy security solutions from Tyco Integrated Security, call Ryan Loughin at 888.446.7781, or visit www.tycois.com/petrochemical

About Tyco Integrated Security

Tyco Integrated Security has a Petro-Chem & Energy Solutions Group dedicated to serving the petrochemical industry. This team 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. Tyco Integrated Security 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. Tyco Integrated Security is a unit of Tyco International, the world's largest electronic security provider. In North America, Tyco Integrated Security provides electronic security services to nearly 500,000 commercial and government customers. Tyco Integrated Security's total security solutions include intrusion, fire protection, video systems, access control, mission critical monitoring, electronic article surveillance, radio frequency identification (RFID) and integrated systems. Tyco Integrated Security's government and commercial customers include a majority of the nation's Fortune 500 companies, all U.S. federal courthouses, over 70 mid-to-large airports and 13 of the top 20 global petrochemical and energy companies. Headquartered in Boca Raton, Florida, Tyco Integrated Security has more than 10,000 employees at approximately 220 locations in the U.S. and Canada. Tyco Integrated Security's services go beyond the installation of security systems. Tyco Integrated Security is SAFETY Act certified and designated for Electronic Security Services from the U.S. Department of Homeland Security.