



Helpful Tips for Completing a Chemical Facility Anti-Terrorism Standards (CFATS) Site Security Plan

Pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS), thousands of Site Security Plans (SSPs) have been drafted by high-risk chemical facilities and submitted to the Department of Homeland Security (DHS) for review and authorization. Additionally, DHS has conducted pre-authorization inspections at some facilities as a means of reviewing submitted SSPs and then providing the facility with additional time to refine the SSP submittal to achieve authorization. As part of the process of reviewing the SSPs and in response to questions from the regulated community, DHS has identified several areas where additional clarity could benefit the development and review of an SSP, including:

1. Appropriate Level of Detail
2. Identifying Specific “Assets” and “Systems”
3. Security Measures Appropriate to Specified Risk Levels
4. Facility-Wide v. Asset-Specific Security Measures
5. Year-Round View

Tip 1: Appropriate Level of Detail

An SSP must include sufficient detail to allow DHS to exercise its responsibility to determine whether the SSP satisfies the CFATS risk-based performance standards (RBPS). To date, many of the SSPs submitted have provided simple Yes or No answers (or similarly brief, non-descriptive responses) to many questions in the CSAT SSP application. Such answers typically do not provide enough information for DHS to make an informed judgment on whether the facility’s security measures satisfy the applicable RBPS.

For example, in responding to questions about RBPS 1 (Restrict Area Perimeter), if a facility simply says that it has a fence, but provides no additional details, DHS has no way of determining how effective the fence would be in securing the facility’s perimeter at the applicable tier. Without additional relevant details (e.g., the height and construction material, whether it has barbed wire, whether there is a clear zone, etc.), DHS is unable to determine whether the fence adequately satisfies RBPS 1.

Facilities can use the SSP text boxes to explain and provide details about existing security measures identified to meet the RBPS. The text boxes can also be used to describe planned security measures and procedures that will provide DHS with sufficient information to review and evaluate the SSP efficiently and promptly.

Tip 2: Identifying Specific “Assets” and “Systems”

For purposes of an SSP, “asset” generally means:

any “on-site or off-site activities; processes; systems; subsystems; buildings or infrastructure; rooms; capacities; ... personnel; or response, containment, mitigation, resiliency, or redundancy capabilities that support the storage, handling, processing, monitoring, inventory/shipping, security, and/or safety of the facility’s chemicals, including chemicals of interest.” (See p. 16 of the DHS Risk-Based Performance Standards Guidance document, May 2009;
http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf)

In addition to COI-specific assets (see Tip 3), SSP assets could include non-COI processes and operations that are essential to the functioning and security of the facility as a whole or of a specific asset. Facility-wide assets could include:

- Utility systems (e.g., power and water)
- Training programs
- Guards
- Inventory control systems
- CCTV
- Intrusion-detection systems
- Escort policies
- Inventory controls
- Background screening
- Shipping and receiving processes

Assets critical to a COI-specific asset might include:

- Process control systems
- Refrigeration systems
- Water curtains
- Nitrogen blankets
- Back-up power systems
- Fail-safe controls
- Anything necessary to maintain the systems critical to a COI-specific asset

When such critical auxiliary processes and operations have not been identified and adequately described, DHS has been unable to adequately evaluate some submitted SSPs. Accordingly, DHS suggests that facilities developing their SSPs consider identifying all systems critical to the overall security and operations of the facility along with any COI-specific assets. For example, a facility may want to ask itself: What processes and protections are in place to help ensure that this facility and its critical assets can function reliably and without undue risk of component or system failure or compromise?

One technique facilities may want to consider for identifying and describing such non-COI-specific assets would be to:

1. Evaluate each of the attack scenarios (e.g., VBIED, Assault Team, Theft) suggested in the RBPS Guidance document (at p. 15) that is potentially applicable to the security risk issues specified in the facility’s final tiering letter, as well as any other plausible attack scenarios that the facility has identified; and then
2. Identify the infrastructure elements, components, systems, people, procedures, safeguards, etc., that could prevent, mitigate or minimize the consequences or likelihood of success of the type of attack that could cause a worst-case security event (e.g., catastrophic release or successful theft of the facility’s COI).

Having identified its relevant assets, a facility might then group these assets in its SSP into “systems” that share:

- A common role or group of roles in the facility’s security system;
- A common set of dependencies on utilities, maintenance, etc.; or
- A common management plan or set of operating parameters.

For example:

1. An SSP could address the security measures related to its perimeter in terms of a system of assets such as fences, gates, wire, lighting, and clear zones. →
2. Within such a “system,” a facility might also want to identify several types of gates as distinct “assets,” since the facility’s operating rules could be different for main gates, employee gates, rail gates, truck gates, fire gates, etc. →
3. Other examples of “systems” could include safety (prevention), operations, cyber, training, response, and mitigation.



Note: While a facility typically should consider off-site assets relevant to the facility’s security, such as off-site water or power generation services, and the potential impact of failure of those systems on the facility’s security risk, the Department understands that the security for those off-site assets is often beyond the control of the facility. In those cases, the facility is not expected to address the security of those assets. However, when designing its security plan, the facility should consider whether to include redundant or alternate systems that could compensate for the failure of off-site assets.



Tip 3:
Security Measures Appropriate to Specified Risk Levels

A facility’s final high-risk notification and tiering letter from DHS specifies a risk tier level for the facility as a whole and typically identifies chemicals of interest (COI) that contributed to that determination. The overall facility tier assignment and the identified COI must, at a minimum, be adequately addressed in the SSP. Specifically, as stated in the final tiering letter:

“All facility-wide security measures, as well as any measures in the SSP relevant to [specified chemicals of highest interest], must correspond to the facility’s final Tier [X] level.”

Where applicable, however, the SSP process allows the facility to include in its SSP some security measures appropriate for a lower tier level than the facility’s overall tier, if those measures are asset-specific and related to COI for which the level of risk, as identified by DHS in the final tiering letter, is below that of the COI(s) of highest interest:

“Asset-specific security measures related to the additional chemicals identified in this letter, however, may correspond either to Tier [X] or to any lower risk levels specified above for those chemicals.”

Thus, any facility that has COI identified by DHS as posing lower risk levels than the facility’s overall risk tier may choose to adopt security measures for assets related to those COI that are less rigorous, and potentially less costly, than measures appropriate for the facility’s overall tier. However, any facility-wide measures that encompass those “lower risk” assets must be appropriate for the overall facility tier level (i.e., perimeter fencing at a site with Tier 1 assets would have to meet Tier 1 standards even if Tier 2 assets are also being secured at the site).

Tip 4: **Facility-Wide v. Asset-Specific Security Measures**

CFATS provides significant discretion to high-risk facilities when they choose to adopt any of the following:

- Security measures for the entire facility;
- Security measures targeted at the asset(s) underlying the facility's security risk level; or
- Some combination of the two.

This flexibility allows a facility to develop and submit an SSP that reflects appropriate facility-wide and asset-specific security measures.

To date, many facilities have treated the entire site as a single asset rather than taking advantage of the ability to identify and describe specific assets – such as an asset with a different risk tier than the facility's overall tier level. If the SSP identifies the entire facility as the sole asset, DHS will expect all security measures identified in the SSP to be in effect for the entire facility and to meet the standards for the tier level applicable to the facility as a whole. While this may be an appropriate approach for some facilities (e.g., a small facility with a single building and a single chemical of interest), it may lead to unnecessary difficulties for other, more complex types of facilities.

In many cases, an SSP that failed to identify discrete assets has resulted in a difficult SSP review process; especially if the SSP also lacked other relevant details (see Tip 1). When a facility had numerous, potentially significant assets and failed to identify them (or otherwise fails to provide important details), DHS has lacked sufficient information to complete its review and has been unable to authorize or approve the SSP. In some cases, this may result in DHS issuing notices of deficiencies or notices of disapproval for the SSPs, potentially leading to enforcement action under CFATS.

Tip 5: **Year-Round View**

If the SSP only addresses the facility's operations and security measures for an unreasonably or arbitrarily limited portion of the year, it may not provide enough information for DHS to determine if the SSP satisfies the applicable standards on a year-round basis or under uncommon but not unforeseeable conditions.

When developing its SSP, a facility should consider all of the relevant and significant activities that go on at the facility throughout the year. This would include:

- Routine day-to-day operations;
- Reasonably-known planned and predictable events (e.g., seasonal/short-term production runs, turnarounds and shutdowns); and
- Unplanned but foreseeable events (e.g., hurricanes, tornados, floods or other natural emergencies) that could significantly affect how the facility's security measures satisfy the CFATS performance standards.

Facilities do not need to consider events that are unrealistic for their specific circumstances (e.g., a Category 3 hurricane in Minnesota) or address every conceivable scenario (e.g., some facilities may never need turnarounds). In certain industries and geographic areas, however, contingency plans already exist for turnarounds, seasonal runs, or extreme weather events. In these cases, it should be relatively straightforward for the facility to address in its SSP the security measures that would be in effect during such events.

Whether or not such contingency plans already exist, the CSAT SSP application allows facilities to supply information related to non-routine but anticipated facility operations under a broad range of conditions. For example:

- The CSAT SSP application provides “Other” text boxes in the questions for specific RBPS that can be used to identify what RBPS-related security measures will be in effect during atypical periods.
- Facilities can use the “Facility Operations” section of the SSP application to describe work shifts for typical operations as well as work shifts for atypical operations.
- Facilities can also use the text boxes to identify by title, date, general content (e.g., “Corporate Hurricane Plan for 2010”) any existing plans or procedures that apply at specified times or under non-routine conditions. If appropriate, DHS can then ask the facility for additional information about such plans.



Note: If a facility feels the text box is insufficient to accurately describe the facility’s activities in response to atypical conditions, it may, but is not required to, upload crisis management, contingency plans, standard operating procedures, or other documents as part of its submission.



Conclusion

DHS is eager to assist facilities in preparing the most appropriate SSPs for their circumstances. We recognize that approvable SSPs can take a considerable, coordinated effort from facility experts to develop, construct, and accurately complete, especially for the more complex covered facilities. Facilities should allow sufficient time for their SSP planners, preparers, and submitters to thoroughly evaluate the processes and operations at the facility so that they can adequately answer the SSP questions and address issues like those discussed above. This coordination will streamline and improve the completion of the SSP.

DHS provides numerous resources to assist facilities in developing and submitting their SSPs and we encourage facilities to take full advantage of those resources. These include:

- The CFATS Help Desk: (866) 323-2957 or csat@dhs.gov;
- A cadre of trained chemical security inspectors that can provide compliance assistance visits;
- A comprehensive, searchable set of Frequently Asked Questions (FAQ) and other resource materials in our Knowledge Center at [http://csat-help.dhs.gov/pls/apex/f?p=100:1:2439979364736107](http://csat-help.dhs.gov/pls/apex/f?p=100:1:2439979364736107;);
- An active outreach program;
- Webinars on completing the SSP and other CSAT tools; and
- A full staff at headquarters to assist with your questions on the CFATS process.

DHS also benefits from hearing your questions and concerns, so let us know how we can help. The more feedback DHS receives, the more DHS can continue to refine and improve the tools, guidance, and information we provide to the regulated community.

To request a Compliance Assistance Visit, outreach presentation or to use other web tools:

http://www.dhs.gov/files/programs/gc_1169501486179.shtm