ChemicalProcessing.com
Leadership • Expertise • Innovation • Interactive

Such an approach may save time and money and provide better protection from all kinds of threats.

By Frank Pisciotta, Business Protection Specialists

The U. S. Department of Homeland Security (DHS) now has assigned sites covered by the Chemical Facilities Anti-Terrorism Standards (CFATS) into one of four risk-based tiers (for more on CFATS, see "Defuse CFATS Challenges." The tier assignment will drive specific security standards that facilities must implement to comply with the regulation.

Within 120 days of receiving its tier notification letter, a site must communicate the elements of its site security plan (SSP) to DHS for administrative approval. This must outline how it will meet the 18 risk-based performance standards (RBPS).

CFATS compliance likely will incur a substantial cost. Based on nearly 20 preliminary engineering studies, estimates have ranged from $500,000 to $2 million per site.

Using an alternative security program (ASP) for the SSP offers several potential benefits — including an initial saving of staff time and thousands of dollars. In addition, an ASP may provide an overall better security posture against the entire spectrum of threats, not just those from terrorism. So, here, we'll:

• look at possible advantages of preparing an ASP;
• provide a model outline for an operational SSP that can be used in addition to, or as a substitute for filing, an online SSP via the DHS Chemical Security Assessment Tool (CSAT) software;
• illustrate key decisions for determining an appropriate strategy for meeting the RBPS;
• point up the importance of involving law enforcement in the gap analysis process as part of the site's security planning process; and
• discuss a potential challenge for small- to mid-size companies.

SSP Options
The regulation stipulates three basic requirements for a SSP:

1. addressing weaknesses identified in the facility's security vulnerability assessment (SVA) and identifying and describing security measures to handle each;
2. specifying how selected security measures deal with applicable RBPS and potential modes of terrorist attacks; and
3. delineating how measures will meet or exceed each applicable performance standard for the facility's assigned tier.

A site can provide information on its SSP to DHS in one of two ways.

The first is via the DHS's Chemical Security Assessment Tool (CSAT) software, similar to that used by most sites to file their SVA. Filing the SSP online involves hundreds of pages of questions and answers. This

process is time-consuming and requires a great deal of upfront data collection before sitting down at the computer. Another significant downside is that there won't be any output from the CSAT software that subsequently can serve as an operational security plan. Such a plan is necessary to guide security and other employees as they meet the security commitments on a day-to-day basis. So, the site still will have the task of developing this plan.

What Type of Physical Security Is Right For Your Site?

Performance metrics associated with the physical security elements of the RBPS likely will result in the greatest cost expenditure. Facilities can choose one of two physical security approaches — focusing either on the perimeter or critical assets. The most appropriate decision depends upon the unique characteristics of the site.

For example, consider a recent study for a mining operation covering more than 11,000 acres. Its critical assets needing protection are located in a 250 ft. × 400 ft. area. So, it makes most sense to target the security design on that small area rather than trying to provide protection for the entire 11,000 acres. Compliance could be achieved with a much lower expenditure.

In contrast, large sites with widely spread out critical assets may have to apply security measures such as intrusion detection, vehicle barriers, surveillance and access control measures to their perimeters.

So, evaluate each facility on a case-by-case basis.

Start by identifying the location of critical assets that must be protected (as defined in a facility's SVA). Designers must use experience and common sense to determine the best way to, among other things:

• keep vehicles away from the critical assets;

Additionally, the online SSP requests a substantial amount of detail about physical security such as the types of access control measures, door hardware, camera types and lighting levels in various parts of the site. Sites likely will need a qualified security professional to help collect these data and prepare them for online submission. That person either can be an in-house or external resource — but ensure that any outside person you use is Chemical-terrorism Vulnerability Information (CVI) certified before any information exchange takes place. It's not difficult to achieve CVI certification; it can be done online.

An ASP also is acceptable for communicating the SSP to DHS. This alternative to online submission may make a lot more sense for some organizations and cost significantly less to implement. This concept is similar to that of the ASP that Tier Four sites could submit as part of the SVA process but applies to all facilities' SSP requirement. We recommend that companies consider this approach, particularly if they have a number of regulated sites.

Organizations with multiple sites can prepare a model corporate ASP. This then can be amended to meet the unique requirements of each regulated site and submitted to meet the SSP requirement, creating additional efficiencies.

A security program that's sophisticated enough to address terrorism demands good documentation — to maintain continuity as personnel changes occur at a facility. According to one chemical industry trade association, "to sustain a consistent and reliable security program over time, companies must document the key elements of their program. Consistency and reliability will translate into a more secure workplace and community."

In addition, a CFATS security program requires substantial training for people with security duties, other employees and even contractors. Such programs also need close coordination with local law enforcement agencies.

Table 1 outlines the contents of a typical security plan. Whether a

• control access from unauthorized persons;

• provide a means to detect unauthorized access attempts; and

• establish a way to assess alarms in a timely manner.

While generally more expensive, the perimeter-based approach does have an upside from the security effectiveness standpoint. In theory, such an approach, if effectively designed, likely will detect an unauthorized access attempt earlier — providing more time for a facility and local law enforcement to respond to interdict a terrorist attack.

You should assess a number of factors when developing a physical security design to comply with the RBPS. The best advice is to carefully consider the results required in your security program, use a competent independent designer (i.e., one not tied to a vendor of security products or services), and determine the appropriate staging plan to intelligently implement physical security measures over time.

facility elects to prepare an operational security plan after filing online via CSAT or to use it as a time- and cost-savings initiative to submit as an ASP, the elements remain the same.

A properly prepared security plan satisfies a fundamental business need to address the full spectrum of threats, not just those from terrorism. In many cases, other risks (i.e., theft, fraud, workplace violence, product pilferage, etc.) represent more likely worst-case scenarios. Consequently, a comprehensive security plan may do more to improve an organization's security posture and bottom line than a plan focused solely on terrorism. In some cases, the failure to properly predict and manage risks can lead to unforeseen liability for organizations.

Preparing the Plan

A baseline plan to meet operational and regulatory requirements always is easier to derive from a completed gap analysis for existing conditions. These conditions are based on specific scenarios the facility must address, which are determined by the chemical(s) on site. One way to prepare a gap analysis is to document existing conditions at the site against the metrics published in the DHS RBPS. That document can be found at www.dhs.gov/xprevprot /programs/gc_1224871388487.shtm.

Each of the four tiers requires a gap analysis tool. It could be expanded to cover all performance metrics in a facility's assigned tier as listed in the October 2008 draft RBPS document (pp. 27–127). This document may undergo some minor revisions; a summary of the changes between that draft and the final version will be posted at www.securingpeople.com.

A key decision that must be made when developing the strategy for an operational security plan is whether the physical security defense plan will emphasize the facility's perimeter or will take a more asset-based approach. An asset-based approach may require a greater investment in barriers and technical measures inside the facility where critical assets are housed. However, depending on the site's size and concentration of critical assets, it

		TITLE	DHS CFATS RISK-BASED PERFORMANCE STANDARD	NOTES
		Leadership commitment	• Officials and organization (RBPS 17)	Defines security organization to manage criminal/terrorist risks.
2		Analysis of threats, vulnerabilities and consequences	• Specific threats, vulnerabilities and risk (RBPS 14)	Identifies risk based on assessment of threat. Requires ongoing mechanisms to monitor for changes in dynamic threats (see RBPS 15 and 16).
3		Implementation of security measures	• Perimeter security (RBPS 1) • Securing site assets (RBPS 2) • Screen and control access (RBPS 3) • Deter, detect and delay (RBPS 4) • Shipping and receiving (RBPS 5) • Theft and diversion (RBPS 6) • Sabotage (RBPS 7) • Personnel Surety (RBPS 12)	Meets the bulk of operational security requirements to safeguard people, assets and information. Requires implementing baseline security measures in normal threat conditions.
4		Information and cyber security	• Cyber security (RBPS 8)	
5		Documentation	• Records (RBPS 18)	
6		Training, drills and guidance	• Training (RBPS 11)	
7		Communications, dialogue and information exchange	• Reporting of significant security incidents (RBPS 15 — partial) • Significant security incidents and suspicious activities (RBPS 16 — partial)	
8		Response to security threats	• Elevated threats (RBPS 13)	Defines measures that are implemented if DHS elevates threat condition or when threats are directed at a specific organization.
9		Response to security incidents	• Response (RBPS 9) • Reporting of significant security incidents (RBPS 15 — partial) • Significant security incidents and suspicious activities (RBPS 16 — partial)	
10		Audits/third-party verification	• Monitoring (RBPS 10 — partial)	

may be far more cost-effective to channel investments to specific areas of the facility (see sidebar).

Table 1. This model uses the security management systems cited in the Responsible Care Code of Management Practices of the American Chemistry Council (ACC). If a site has adopted an operational security plan consistent with the ACC model, risk-based performance standards should align well with that model. Other models for security management systems also are available.

Involving local law enforcement agencies is an important aspect of gap analysis and security planning. In a survey of more than a dozen regulated facilities in rural areas of the U.S., none of the responding Sheriff's Departments was aware of the requirement for CVI training. As a result, nobody in those agencies has a CVI certificate that would have allowed the site and its consultant to discuss regulatory requirements or share detailed security-planning information for the betterment of the security program.

A review of the National Sheriff's Association Web site reveals no information on CFATS or CVI. This suggests that additional communication is needed between DHS and the local law enforcement community. Until then, sites must address the need for CVI certification on a case-by-case basis. Most agencies encountered to date have been willing to explore and undergo the online DHS training. Keep in mind, however, that it's illegal for sites to involve external authorities in detailed planning until CVI certification can be proven.

An additional challenge for small- to mid-sized companies is to determine exactly how all of this work to implement the regulation will get done. Typically, this size organization assigns security to non-security professionals with other responsibilities — we call them facility security officers; they may never have received training in security management. A closely related regulation, the Marine Transportation Security Act, stipulates the skills and competencies required of a facility security officer. My firm now is training CFATS facility security officers to close the gap left open by the lack of specific requirements in the regulation.

The Clock Is Ticking
Regulated chemical facilities now must make a SSP commitment to DHS. Corporate management may want to consider developing an operational security plan to serve as a substitute for the online filing of a CSAT SSP. At a minimum, we recommend having a documented security plan in place by the time a DHS inspector arrives for the on-site inspection. The ASP approach can help facility and security managers achieve this goal.

Frank Pisciotta is president of Business Protection Specialists, Canandaigua, N.Y., and is a Certified Security Consultant. E-mail him at fp@securingpeople.com.

Search ChemicalProcessing.com