CEP Chemical Engineering Progress

AIChE American Institute of Chemical Engineers

Three Park Avenue
New York, NY
10016-5991
www.aiche.org

Facility Management Insecurity

The Synthetic Organic Chemical Manufacturers Association (SOCMA) and the U.S. Dept. of Homeland Security (DHS) recently hosted 350 attendees at the 2008 Chemical Sector Security Summit. Attending engineers and managers listened to speakers and participated in workshops that explained the complexities of the Chemical Facility Anti-Terrorism Standards (CFATS).

CEP has covered this topic twice this year — in January's Ask the Experts ("Complying with Anti-Terrorism Standards," p. 26), and in May ("Plant Security Remains a Moving Target," pp. 6–7), so it made sense to followup and observe.

Post-presentation Q&A sessions revealed that many are confused by the new regulations and are therefore anxious about compliance. Consider the perspective of the attendees. The event took place six months after all vulnerable facilities submitted their Top Screen registrations. It was also about two months after they were supposed to receive letters notifying them of their designated tier (Tier 1 to Tier 4, or none). Those assigned to Tier 1 have only 90 days to submit a security vulnerability assessment (SVA) to DHS (Tier 4 facilities have 180 days). Pressed for time, the attendees had good reason to worry.

Speakers covered the 19 CFATS-initiated risk-based performance standards (RBPSs) for site security plans (SSPs), but several attendees still had trouble understanding when background checks are required. They are mandatory for anyone with the authority to tour a facility unescorted, but not for escorted visitors/contractors, nor for those with access to traveling assets at offsite railcar swap stations. No guidelines specify how often someone's identity should be verified. No automatic system is set up with the DHS, as the responsibility lies with the facility.

Another panel fielded audience questions on how sensitive information should be protected. They explained when data should be treated as chemical-terrorism vulnerability information (CVI), protected critical infrastructure information (PCII), and/or sensitive security information (SSI). Just because information is regulated by a DHS process does not necessarily make it protected as CVI. For example, a facility manager submits materials as part of the initial Top Screen process, and receives a letter indicating that the facility is not "tiered" at this time. However, seeking further input on security, this manager submits an SVA anyway. In this scenario, the Top Screen materials are classified as CVI, but the optional SVA materials are not. A revised CVI manual was due out in late August. It should clarify when data become CVI-protected and when they do not.

If an inspector (for example, one operating under the Public Health Services Act) wishes to see a tiered facility, he/she must be an "authorized user" (as defined by DHS). Problems arise when the inspector claims to have clearance but the manager has no way to verify that claim. The DHS expects (but does not mandate) the facility to contact it prior to the scheduled inspection for clarification.

An attendee received applause when he called on the panelists to give firmer answers, saying that many facility managers are afraid to deny an inspector access because the scope of the inspection may be expanded in retaliation. The DHS assured the audience that those who have taken reasonable steps at verification of an inspector's credentials will be afforded protection.

These examples cover only two sessions at one conference. It is very likely that many other issues will remain unresolved when the deadlines pass. The DHS should provide leeway for those who make good-faith efforts to meet these new regulations but fail to do so because of ambiguous guidelines.

Matthew McKeon-Slattery, Assistant Editor