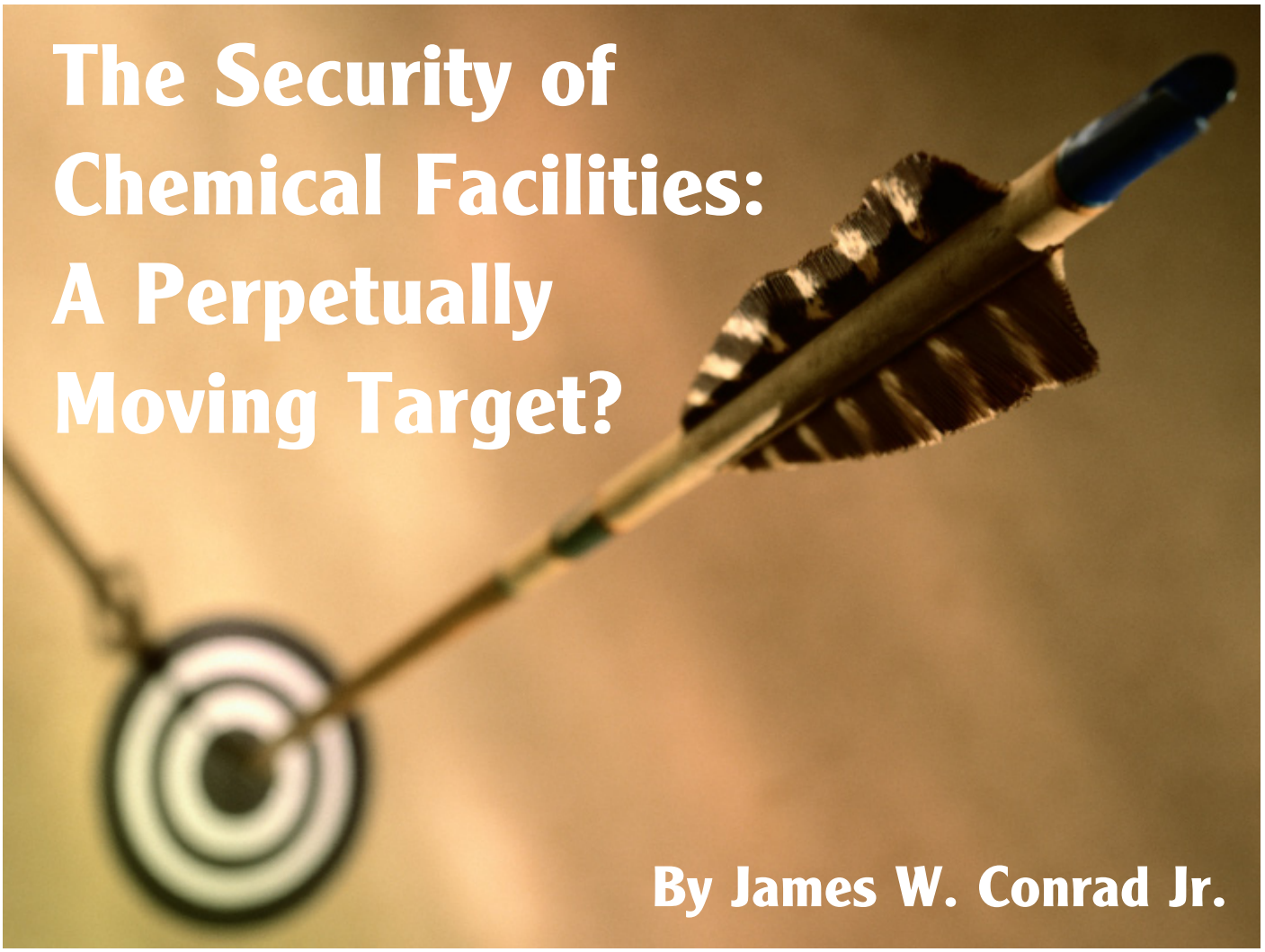

# The Security of Chemical Facilities: A Perpetually Moving Target?

By James W. Conrad Jr.

More than six years after 9/11, the Department of Homeland Security (DHS) is deeply enmeshed in designing and implementing a novel program, based on risk assessment and performance standards, to regulate the security of chemical facilities; to use a popular DHS metaphor, the department is "building the airplane as they fly it." Because five years of stalemate preceded the enactment, in October 2006, of the legislation authorizing this nascent program, one might reasonably expect Congress to turn to other security topics that it has yet to resolve. Instead, legislators are continuing to do battle on the field of chemical facility security. The fighting has continued most fiercely over the no-man's land of "inherently safer technology," although new fronts have opened up over the adequacy of DHS' current authority and its pre-emptive effect. DHS and industry leaders are united, to some extent, by fear of what Congress' next bill might look like and are awkwardly engaged in a mutually skeptical alliance, seeking to make the current program a success for both sides.

This article begins by briefly recounting the five years of conflict that resulted in the current law, then describes the program that DHS is building to implement that law. Next, the discussion summarizes currently pending legislation and the issues that continue to motivate Congress. Finally, the article explores whether the features that make the current program innovative can survive, or whether the security of chemical facilities is likely to become just another "environmental" program—only worse.

## The Five-Year War

Barely a month after 9/11, then-Sen. Jon Corzine (D-N.J.) introduced the Chemical Security Act of 2001 (S. 1602). The bill was nominally directed at enhancing the security of chemical plants—"nominally," because the Corzine bill contained not one word about security in the conventionally understood sense of the term: actions designed to detect, deter, and delay bad actors. Instead, the bill was focused on what has come to be called "inherently safer technology" (IST).

First given a name several decades ago by process safety experts within the chemical industry, "inherent safety" means eliminating a hazard when a process is designed in order to obviate the need to manage the hazard afterward—for example, inflating blimps with helium rather than hydrogen. Deceptively simple in concept, inherent safety can be highly complicated in application, especially as one strives to avoid merely shifting a risk elsewhere or unwittingly creating a new one. And although inherent safety has

become standard practice within the chemical industry and a basic element of chemical engineering education, there is as yet no consensus on the methodology to be used to compare the inherent safety of multiple approaches. And in some cases, the exercise is ultimately subjective or arbitrary—for example, how should one weigh an explosion hazard against a possible cancer hazard? To add to the problem, environmental activists have seized on the label of inherently safer technology as a way to promote the elimination of particularly hazardous chemicals like chlorine. As a result, the chemical industry has been resolutely opposed to government requirements related to inherent safety, especially if they empower government officials to second-guess decisions made by process engineers.

The premise of Corzine's bill was that mandatory IST could require chemical operations to eliminate or reduce their stocks of hazardous chemicals to the point that the materials would no longer be attractive targets for terrorists. That the bill would have given oversight of what had traditionally been understood as a law enforcement function to the U.S. Environmental Protection Agency (EPA)—an agency presumably sympathetic to the cause of eliminating hazardous chemicals—only compounded the bill's problems in the industry's eyes.

Corzine's bill was hotly contested, as were subsequent bills introduced by other senators and representatives in the intervening years. Even though the extent of the disagreement narrowed with time—after DHS was established in 2003, all serious bills on the topic assigned primary jurisdiction to DHS rather than to EPA—IST remained the single issue on which neither side would compromise. Early on, in 2002, Congress was able to pass legislation addressing security at two categories of facilities that could contain chemicals: maritime facilities and public drinking water systems. But these were special cases; the drinking water plants sought regulation by EPA because the oversight came with money for implementation, and maritime facilities were swept up in much larger legislation involving port security (which, coincidentally, also promised grant money). But progress on chemical plants per se proved elusive for five years.

Finally, as the 2006 congressional elections drew near, the fear of being criticized for having done nothing and the uncertain prospect of changes in the control of Congress led that body and DHS to strike a deal on a page and a half of text in the DHS appropriations bill for fiscal year 2007. (Pub. L. No. 109-295, enacted Oct. 4, 2006). That provision (§ 550 of the bill) is now being implemented as the Chemical Facility Anti-Terrorism Standards or CFATS rule, which is discussed next. Whether CFATS will prove sufficient to forestall further legislation will be addressed after that discussion.

## Chemical Facility Anti-Terrorism Standards

Section 550 requires DHS to issue implementing rules within six months—without notice and comment. To its credit, DHS managed to publish a "draft" rule for comment in a few months (71 Fed. Reg. 78276 (Dec. 28, 2006)), then issued an "interim final rule" (IFR) on April 9, 2007 (72 Fed. Reg. 17688, to be codified at 6 C.F.R., part 27). To meet its six-month deadline, DHS essentially punted the most complicated issue—coverage—to a subsequent rule, Appendix A to the IFR, which was published as a final rule on Nov. 20, 2007 (72 Fed. Reg. 65396), and became effective that day.

### *Applicability*

Section 550 applies to chemical facilities that "present high levels of security risk." The IFR's definition of "chemical facility" is extremely broad: "any establishment that possesses, or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by [DHS] to be potentially dangerous or that meets other risk-related criteria identified by [DHS]." Under the IFR, DHS uses a Web-based screening tool called "Top-Screen" to determine if a chemical facility is a high-risk establishment. If DHS concludes that the facility is, such a "covered facility" is then subject to other requirements of the IFR.[1]

The Appendix A rule contains a table that lists some 335 "chemicals of interest" and sets a "screening threshold quantity" for each chemical for each applicable type of hazard scenario, or "security issue." (There are seven security issues; three involve release of a chemical, three involve theft or diversion, and one involves sabotage/contamination.) In general, if a facility possesses a chemical listed in Appendix A at or above one of the screening threshold quantities, the facility must complete and submit a Top-Screen report. According to DHS, some 30,000 facilities completed Top-Screen reports by the initial deadline of Jan. 22, 2008. (Drinking water and maritime facilities regulated under the 2002 legislation are exempt, as are wastewater treatment plants, even though security at these is not regulated by any federal agency.)

### *Security Vulnerability Assessments*

The Department of Homeland Security has consistently stated that it expects to identify between 5,000 and 8,000 facilities as high-risk establishments. The department will provisionally assign each such facility to one of four risk-based tiers, with Tier 1 being the highest risk. (DHS has classified the criteria for making determinations of "high risk" and tier assignments.) The department will appoint a "coordinating official" to see that the program is applied uniformly and fairly. Facilities that question their status as high-risk establishments or their tier assignments can seek a "consultation" with this official. In all likelihood, notification letters will be mailed to facilities while this article is in press.

The first compliance obligation of covered facilities will be to conduct a security vulnerability assessment (SVA) and to file it with DHS. DHS is working on an electronic SVA tool that will be posted on their Web site. Facilities in Tiers 1–3 are required to use that tool, and once it is posted, they will have 90, 120, and 150 days, respectively, to complete and file their assessments. Tier 4 sites must also complete an SVA (within 180 days), but they may use any one of several methodologies approved by DHS.

### *Site Security Plans*

Once DHS approves a facility's SVA submission (which supposedly will happen within 60 days), the facility will have 120 days to develop a site security plan (SSP) and submit it to the DHS Web site. The SSP must describe the facility's security measures and explain how they address both the vulnerabilities identified in the SVA and the applicable "risk-based performance standards" (which are discussed below). Upon its preliminary approval of the SSP, DHS will issue the facility a Letter of Authorization. After DHS inspectors have visited the facility and found it to be in compliance, the department will issue it a Letter of Approval. If a facility believes that it will not be able to fully implement its plan by the inspection date, the facility's representative can discuss the matter with DHS.

Facilities designated as Tier 1 and Tier 2 facilities must update the Top-Screen report, SVA, and SSP every two years. Those in Tiers 3 and 4 are on a three-year review schedule. In addition, facilities making modifications that they believe will reduce their risk profile have informal and formal opportunities to seek DHS' agreement. Conversely, facilities that materially increase their risk profile must resubmit Top-Screen reports within 60 days of making the modification.

### *Risk-Based Performance Standards*

Chemical facilities are diverse, ranging from huge complexes covering many square miles to small batch operations. The facilities may be located in remote areas or in densely populated urban areas. They may contain vastly differing amounts of chemicals of differing degrees of security sensitivity. What's more, there usually are multiple ways that a facility can secure itself from terrorists. To encompass this diversity in a sensible way, § 550 adopts an approach that is based on risk and performance, and this is the rule's most innovative feature. Rather than specifying (or authorizing DHS to specify) blanket or particular security measures, § 550 states that DHS

> shall issue interim final regulations establishing risk-based performance standards for security of chemical facilities … [and t]hat such regulations shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility.

To implement this language, the IFR establishes 19 categories of risk-based security performance standards (RBPS) that are intended to become increasingly demanding as a facility moves from a Tier 4 designation to Tier 1. (Examples include restricting the facility perimeter; deterring, detecting, and delaying potential attackers; training personnel; and assessing the backgrounds of personnel.) DHS will shortly issue a nonbinding guidance document that provides the department's interpretation of what the RBPS require of facilities in the various tiers.

### *Inherent Safety*

The portion of § 550 quoted above continues with this language: "The [s]ecretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the [s]ecretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section." The upshot of this language is that, even though a facility has to meet the applicable RBPS, it has the discretion to choose the measures that it will adopt to do so. It follows from this statement that DHS cannot require implementation of IST. DHS has also expressed the view that it cannot set performance standards in such a way as to require IST (or any other security measure) as a practical matter (for example, by setting a standard of "no offsite impact in the event of a successful terrorist attack"). However, facilities are free to consider IST options to reduce risk and thus meet a performance standard, move to a lower tier, or stop being designated as high-risk establishments.[2] DHS staffers have indicated that the department may not agree to recategorize a facility as no longer high-risk or move it to a lower tier based on IST if the proposal would shift risk off-site, otherwise would not actually reduce the risk, or would compromise security.

### *Background Checks and Personnel Issues*

The IFR requires background checks and identification for all facility employees, contractors, and other visitors who have unescorted access to restricted areas and critical assets at a facility. The facility is responsible for determining what criminal background findings would disqualify a person and for checking the criminal background and immigration status of these individuals. DHS intends to establish, in 2009, a fifth Web-based application that will enable employers to submit names to the department through CSAT for automated evaluation against the National Terrorist Screening Database.

Neither § 550 nor the IFR establishes a system that whistle-blowers can use, but DHS has stated that it intends to establish a telephone line through which employees and other individuals can submit their concerns about security at the facility. Nor does either rule mandate participation by any particular types of employees in the compliance and implementation processes. Organized labor would like to see more requirements on both scores.

### *Inspections and Enforcement*

Section 550 requires DHS to review and approve each SVA and SSP and also requires the department to inspect covered facilities. If DHS finds a violation, the department must give the facility a clear written explanation of deficiencies and an opportunity for consultation and may issue the facility an order to comply by a date that DHS determines is "appropriate under the circumstances." If the facility does not comply with the order, DHS may impose a civil administrative penalty of up to $25,000 per violation and may also issue an order for the facility to cease operation until it complies with the order.

The IFR establishes administrative adjudication rules

and provides for an appeals process to the undersecretary of DHS. The undersecretary's decision is judicially reviewable, but given the amount of discretion that the statute and the IFR accord to DHS regarding the security measures required at a facility, it seems likely that courts will defer heavily to the department.

The initial focus of DHS' compliance efforts will be reviewing SVAs and SSPs, which will be a centralized, paper (documentary) process. Actual site visits will not begin until after the initial batch of SSPs has been approved. This is just as well, because DHS currently has fewer than 40 field inspectors, all of whom were borrowed from Federal Protective Services for a three-year detail that is mostly over. Even though these jobs will be posted and filled as permanent DHS inspector positions, in the coming years the department will face challenges in fielding enough inspectors to meet its inspection obligations. As a result, DHS has raised the prospect of a future rulemaking to authorize the use of third-party auditors to conduct inspections.

***Protection of Information***

Advocates of the public's right to know and of open government have complained mightily that, although the 9/11 Commission called for greater information sharing and a move away from the "need-to-know" culture, Congress and DHS have been steadily creating new regimes for the protection of information that has been gathered—most prominently DHS' "protected critical infrastructure information" (PCII) rules and broadly expanded rules regarding "sensitive security information" (SSI) established by the Department of Homeland Security and the Department of Transportation.[3] Section 550 struck an ambiguous note on this score by providing that information developed pursuant to the rule must be "given protections from public disclosure consistent with" the SSI rules, except that, in enforcement cases, information is to be treated as if it is classified.

Rather than narrowly amending the SSI rules, however, in Subpart D of CFATS DHS established yet another category of information protection: "chemical-terrorism vulnerability information" (CVI). Even though, on their face, the CVI rules look very similar to the SSI rules, DHS has issued a controversial CVI "procedural manual" that is more restrictive than the Coast Guard's current SSI guidance, particularly as regards a company's treatment of its own information. *See* www.dhs.gov/xprevprot/programs/gc_1181835547413.shtm. According to the manual, persons entitled by law to have access to CVI must complete DHS training and sign a restrictive nondisclosure agreement before they can be added to the DHS master list of "authorized users." (The SSI rules do not include a similar concept.) Companies are told to maintain detailed tracking logs of who has had access to what CVI and when. Uncertainties abound about how to treat information that facilities have historically generated that now is designated CVI, as well as how to "sanitize" CVI information so that it can be supplied to employees who are not authorized users.

DHS may give a CVI designation to state or local officials who have a need to know, but any state laws dealing with the public's right to know or sunshine laws that might require or allow those officials to release that information are pre-empted. The procedural manual instructs facilities to seek DHS approval before giving information to state or local government officials. State and local officials are quite unhappy with this direction and have been working with DHS to establish a means by which they can have access to CVI directly from the department.

***Pre-emption***

After the concept of inherently safer technology, the most fiercely contested issue in the chemical facility security debate has been the extent to which federal requirements would pre-empt state programs that address the same topic. Only three states have any such program,[4] but the issue has taken on disproportionate importance, mainly because it serves as yet another venue for proponents of IST to promote their cause. The "prescriptive order" issued in New Jersey in 2005 required facilities in specified categories to take IST into account on a one-time basis, although the facilities remained free either to implement IST or to explain to the state why doing so was not feasible. In every other respect, the prescriptive order was actually less demanding than CFATS. Critics of DHS and supporters of IST, however, regularly trumpet New Jersey's "more stringent" program and have made pre-emption the second major battleground in the war over the security of chemical facilities.

Section 550 is silent on the topic. The DHS draft rule contained aggressive language implying that the law "occupied the field" and implicitly pre-empted all state enactments on the subject. After fierce criticism, DHS retreated in its IFR, stating that § 550 pre-empted only state programs that conflict with the federal program. This explanation was still insufficient for its opponents, who succeeded in including, in the FY 2008 omnibus spending law, a provision declaring that § 550 and CFATS did not pre-empt states' requirements governing with the security of chemical facilities unless there was an "actual conflict" between the two. *See* Pub L. No. 110-161, § 534. DHS Secretary Chertoff has stated that DHS has no reason to conclude that any current state programs actually conflict with CFATS.

***The Legislative Struggle Continues***

The price the authorizing committees exacted for allowing § 550 to bypass their jurisdictions was a sunset provision that ends DHS' CFATS authority on Oct. 1, 2009. Although we're barely halfway there, the House Homeland Security Committee has seized upon the sunset provision as the pretext to move aggressively with new legislation that makes several clear changes and numerous potential ones to CFATS. (H.R. 5577, reported from committee on March 6, 2008.) Meanwhile, on March 5, the former chair of the House Energy and Commerce Committee's Environment and Hazardous Materials Subcommittee introduced a bill (H.R. 5533) that would do little more than simply strike the sunset clause from § 550.

Particularly because asserting of jurisdiction is at least as important to both committees as moving a bill through

Congress, it is difficult to predict the future of these bills. But even if neither passes, the next Congress will pick up wherever this Congress leaves off. H.R. 5577 looks a lot more like prior bills and therefore seems more likely to resemble the legislation of the 111th Congress. DHS is striving mightly, however, to establish such a mature and accomplished program that Congress coalesces around the minimalist approach of H.R. 5533. In the meantime, those interested in the debates would benefit by understanding both bills.

***CFATS Integration***

It seems likely that facilities that are designated as Tier 1 facilities under CFATS will have filed their vulnerability assessments and plans by the end of 2008 and may have completed the implementation and inspection process by Oct. 1, 2009, the deadline set by the sunset provision of § 550. These facilities—and the Department of Homeland Security—are thus understandably alarmed at the prospect that they will immediately have to repeat the process or, worse, that Congress might completely redesign the program. The first draft of the committee's proposal that became H.R. 5577 was released in December 2008 and fanned these fears by adopting a Rip Van Winkle approach—referring to § 550 only where the bill repealed it and generally implying that DHS would need to start all over again.

Fortunately, the reported bill states that the "purpose of th[e] [a]ct is to give permanent status" to the CFATS regulations and that those rules "largely address the concerns of Congress with respect to chemical facility security." The bill also declares the sense of Congress that DHS should use "rules, regulations or tools developed for purposes of the CFATS regulations as the [s]ecretary determines are appropriate"—including Appendix A and Top-Screen—to implement the new legislation. Finally, H.R. 5577 authorizes $225 million in each fiscal year from 2010 to 2012 to support implementation of its requirements. Against all this, however, is the fact that the bill would require DHS to undertake a major rulemaking in FY 2009, at the same time that it is implementing CFATS (and a new ammonium nitrate mandate), with no new resources for that period. The result could only be delay and distraction from the department's current mission.

***Scope of the Bill***

One part of H.R. 5577 is much like CFATS: DHS must publish a list of "substances of concern" and "threshold quantities" that implicitly would serve a screening function similar to the one they serve under CFATS. The department then must develop a list of covered chemical facilities, based on factors that largely track those included in CFATS. Facilities are to be assigned to one of at least four risk-based tiers, at least one of which must be "high-risk" facilities.[5]

Unlike the CFATS rule, H.R. 5577 does not exclude wastewater systems, drinking water plants, or maritime facilities. Even though including these systems and facilities makes sense for wastewater facilities, whose security is currently unregulated, it poses a very real threat of duplicative regulation for drinking water plants (where security is currently regulated by EPA under the Safe Drinking Water Act) and maritime facilities (where security is currently regulated by the Coast Guard). The bill says merely that the secretary of DHS is to "work with" the commandant of the Coast Guard (who reports to the DHS secretary) and with EPA to "ensure that requirements under [the competing programs] are non-duplicative and non-contradictory"—language that could well mean little in practice. Congress should require these agencies to issue joint rules under their respective authorities so that they can not leave it to facilities to sort out conflicts that the agencies cannot or will not resolve.

***Requirements of Facilities***

Covered facilities must submit SVAs and SSPs to the Department of Homeland Security. More detailed requirements are specified for SVAs and SSPs that high-risk facilities are required to submit. To assist covered facilities in preparing SVAs, DHS must provide them with "the number of individuals at risk of death" or serious adverse effects from a worst-case terrorist incident at the facility—information that the facilities are unlikely to want to possess. (Under the CFATS rule, DHS keeps these estimates to itself.)

All covered facilities must implement security measures meeting risk-based security performance standards that are tougher for facilities in higher tiers. The list of performance standards tracks the CFATS list and adds two new standards: early warning systems and IST (discussed below). The bill also adds two arguably redundant freestanding requirements for training employees and reporting incidents related to security at the facility.

SVAs from newly regulated high-risk facilities are due three months after the implementing rules are issued (that is, no later than Jan. 1, 2010). SSPs from such facilities are due four months after receiving notice from DHS that the SVA has been approved. These deadlines can be extended for a facility for up to six months. The bill does not specify a deadline for other newly regulated facilities.

Facilities that have already submitted an SVA or SSP by Oct. 1, 2009, "shall be required to submit an addendum … to reflect any additional requirements under this title or the amendments made by this [a]ct." This requirement could amount to the need for facilities to conduct their security vulnerability assessments or develop site security plans all over again.

***Inherently Safer Technology***

H.R. 5577 requires all covered facilities to describe in their SSPs "methods to reduce the consequences of a terrorist attack"—that is, inherently safer technology. High-risk facilities must implement IST if using it—

- "would significantly reduce the risk of death, injury, or serious adverse effects to human health or the environment" from a terrorist release "but would not increase the interim storage of a substance of concern outside the facility or directly result in the creation of a new chemical facility assigned to a high-risk tier … or the assignment of an existing facility to a higher risk tier";

- "can feasibly be incorporated into the operation of the facility"; and
- "would not significantly and demonstrably impair the ability of the owner or operator of the facility to continue the business of the facility at a location within the United States."

The secretary of DHS would decide appeals. The department would also maintain a public clearinghouse of IST information gleaned from facilities.

This IST mandate is by far the most nuanced requirement in any federal bill. H.R. 5577 also attempts to sweeten the pot by authorizing $100 million in FY 2010, $75 million in FY 2011, and $50 million in FY 2012 that the secretary "shall make … available to defray the costs of implementing" IST voluntarily or mandatorily but will give "special consideration" to facilities required to implement IST. It remains to be seen if these accommodations, plus the heat of a presidential campaign, will reduce opposition to the point that an IST mandate can be enacted.

***The Role of Unions***

Perhaps it is not surprising that a bill being considered by a Democratic Congress entitles union representatives—

- to be included in the development of SVAs and SSPs;
- to participate in drills and exercises;
- to be notified of impending "red team exercises" (discussed below);
- to participate in inspections; and
- to receive copies of a facility's SVA and SSP.

The last point is bound to be a subject of contention, given the extraordinary sensitivity of these documents, especially SVAs. What's more, even though union representatives must "ensure that any such [documents are] handled and secured appropriately," union personnel face no sanctions if mishandling occurs.

***Red Team Exercises***

Selected high-risk facilities must undergo a "red team exercise" (a term that is left largely undefined) conducted by DHS within six years of enactment of the legislation. Facilities would get prior notice, and DHS must receive positive confirmation before beginning the exercises. Red team exercises may not compromise the security of a facility during the exercise. Security plans must address vulnerabilities that a red team exercise identifies.

***Security Background Checks***

DHS is required, evidently by Oct. 1, 2009, to issue rules requiring high-risk facilities to conduct security background checks on employees and contractors[6] ("covered individuals") who have access to restricted areas or critical assets or who are determined to require background checks on the basis of risk-based guidance provided by DHS. According to the rules for such checks, which must be conducted at no cost to the individual, a facility is allowed to take an adverse action against a covered individual only "due to" those rules or other DHS pronouncements (1) for the same criminal offenses that apply to applicants for hazmat endorsements or Transportation Worker Identification Credential (TWIC) cards, or (2) for being an illegal alien or a terrorism risk.

The rules must also mandate that facilities establish a "redress" procedure, equivalent to the one required by the TWIC program, for individuals who are recipients of an employer's adverse action as a result of such checks. Covered individuals must receive full wages and benefits until all appeals and waiver procedures have been exhausted. DHS can penalize a facility owner or operator who fails to comply with these rules. The bill also makes it a crime to knowingly misrepresent to any relevant person the scope, application, or meaning of any DHS rules or guidance about background checks.

***Alternative Security Programs***

The Department of Homeland Security can approve alternative security programs for individual facilities or classes of facilities if they meet the requirements stated in the bill.

***Enforcement***

DHS must review all SVAs and SSPs within six months of receipt. Apparently, the department is not required to inspect all facilities—or even all high-risk ones—but it can authorize third parties to review submissions or conduct compliance inspections. Shutdown orders can be issued for failure to comply with a compliance order. Failure to comply with a compliance order also subjects a facility to civil judicial penalties of up to $50,000 per each day of noncompliance.

***Whistle-blowers***

DHS must develop a process for people to submit reports of problems or vulnerabilities at facilities. Companies cannot retaliate against persons who report problems under this process or who engage in a wide variety of other protected actions. Claims of retaliation would be adjudicated by the Department of Labor.

***Pre-emption***

H.R. 5577 confirms that the federal program would not pre-empt state or local requirements related to the security of chemical facilities "unless a direct conflict exists" between those requirements and the bill. It is unclear whether this means something different than the "actual conflict" standard recently established by the FY 2008 omnibus spending bill.

To clarify the statement made earlier—that H.R. 5533 would do "little more" than codify § 550 without the sunset provision—the *only* other thing the legislation would do is to override the actual conflict provision just referenced by stating that § 550 does not pre-empt *any* state action. This language comes from the House's version of the FY 2008 DHS spending bill, and it may well meet the same fate as that language, because of the likelihood that the Department of Homeland Security and regulated facilities

will strenuously oppose that feature of the bill.

***Protection of Information***

H.R. 5577 creates fairly robust information protections, including criminal penalties for government employees who knowingly disclose protected information. As with current law, sensitive information used in enforcement proceedings would be treated as if it was classified. The bill does not address any of the issues that have been raised by the CVI Procedural Manual issued by DHS.

***Voluntary Industry Consensus Standards for Security Training***

In addition to the employee training requirement noted above, DHS is supposed to "support the promulgation" of voluntary industry consensus standards for facility security training. This requirement is problematic both because "promulgate" generally means "issue by rule" and because these standards may be enforceable.

## Conclusion

Opinions rendered by multiple comptrollers general support the view that even bare appropriations to fund the CFATS program after FY 2009 would be sufficient congressional action to supersede the sunset clause found in § 550. However, the concept of chemical facility security has proven to be a more alluring target to legislators than chemical plants have thus far proven to be to terrorists. What is more frustrating, the appeal of the concept seems to arise less from how secure these plants actually are than from the ability of legislation to effectuate long-frustrated goals of reducing and eliminating the use of chemicals. Those most interested in accomplishing those goals have an inherent interest, therefore, in belittling accomplishments under the CFATS program—no matter how substantial they may be. The contenders for the Democratic Party's nomination, Sen. Barack Obama of Illinois and Sen. Hillary Rodham Clinton of New York, and Sen. Joseph Lieberman (I-Conn.)—who has been mentioned as presidential hopeful Sen. John McCain's (R-Ariz.) choice to head up the Department of Homeland Security—have all co-sponsored IST legislation at various times. Hence, in 2009, the Department of Homeland Security and the industry will have their work cut out for them.

When the Environmental Protection Agency promulgated the Clean Air Act Risk Management Program rule in 1996, some observers believed that the rule should require facilities to conduct "technology options analyses" to identify inherently safer approaches for chemical processes. EPA declined to do so, stating that process hazard analysis teams—

> regularly suggest viable, effective (and inherently safer) alternatives for risk reduction, which may include features such as inventory reduction, material substitution, and process control changes. These changes are made as opportunities arise, without regulation or adoption of completely new and unproven process technologies. … EPA does not believe that a requirement that sources conduct searches or analyses of alternative processing technologies for new or existing processes will produce additional benefits beyond those accruing to the rule already.[7]

It is instructive that, even when the EPA was headed by Carol Browner, the agency still took a pass on the opportunity to assess—and make judgments about—the inherent safety of potentially thousands of chemical operations. If IST legislation is enacted next year, the Department of Homeland Security will face a task from which even the Environmental Protection Agency has shied away. **TFL**

---

*Jamie Conrad is the principal of Conrad Law and Policy Counsel in Washington, D.C., where he provides regulatory and legislative representation in the areas of homeland security, environmental law, and science policy. From 1993 to 2007, he served as in-house counsel at the American Chemistry Council, the country's largest chemical industry trade association. He received his B.A. from Haverford College and his J.D. from George Washington University School of Law. He can be reached at jamie@conradcounsel.com.*

## Endnotes

[1]Top-Screen is part of a secure Web-based DHS portal called the Chemical Security Assessment Tool or CSAT. The CSAT application, which is how potentially and actually regulated facilities file required reports under CFATS, is one of the major innovations of the rule.

[2]72 Fed. Reg. 17707, 17718.

[3]These rules and the controversies surrounding them are discussed at length in James W. Conrad Jr., *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 ADMIN. L. REV. 715 (Summer 2005).

[4]Maryland and New York have enacted legislation governing security at chemical facilities (see, respectively, Md Env't Code § 7-701 to 7-709 and NY Exec. Law §§ 709–712); New Jersey has issued a "prescriptive order" to specified facilities (*see* State of New Jersey Domestic Security Preparedness Task Force, Domestic Security Preparedness Best Practices at TCPA/DPCC Chemical Sector Facilities, ¶ 5 (Nov. 21, 2005), available at www.acutech-consulting.com/acutech-news/2005/BestPracticesStandarsActonChemicalPlantSecurityNov212005.pdf).

[5]Committee staff members have stated that they intend for the universe of "covered facilities" subject to the bill to be the same as the universe of "high-risk" facilities subject to CFATS. Ideally, the bill would be revised to change the reference to "high risk" to something like "highest risk."

[6]The bill does not address how a facility owner or operator would conduct background checks on contractor employees, whether it could rely on the contractor to do so, or what implications such checking might have under other laws regarding who is such a person's "employer."

[7]61 Fed. Reg. 31699 (June 20, 1996).