

7. CHEMICAL PLANT SECURITY PREVENTING A TERRORIST BHOPAL

There may be no better example of a sector encompassing a large number of high-impact targets than the chemical industry. The industry produces, stores, and transports large quantities of highly toxic agents for a wide range of industrial uses. According to DHS planning scenarios released last spring, a truck bomb detonated at a chlorine plant could cause 17,500 deaths and millions of dollars of damage. These figures are probably conservative. With minimal reconnaissance and the technical knowledge to make a fertilizer bomb, terrorists could kill large numbers of people by targeting one of the thousands of facilities that handle large quantities of highly toxic chemicals in close proximity to our nation's cities and towns.

Preventing such an outcome has relied largely on voluntary measures, most notably adherence by the members of the American Chemistry Council (ACC) to its Responsible Care Security Code. In all, the chemical industry has spent \$2 billion on security since the attacks on September 11, a not unimpressive figure.¹ Yet, due to the voluntary nature of these measures and a lack of oversight by the federal government, the Government Accountability Office (GAO) and outside experts have concluded that the overall level of security in the industry remains inadequate. The Chemical Facility Anti-Terrorism Act of 2005, a bill introduced to the Senate by Senator Susan Collins (R-ME), would go a long way toward improving security in the chemical industry. It sets the stage for the Department of Homeland Security (DHS) to take the kind of smart approach to regulation we advocate here.

The goal of regulating security in the chemical industry should be to reduce or eliminate vulnerabilities rather than to turn every chemical plant into Fort Knox. The Collins bill provides a “tiered” approach to

security, in which companies are placed in tiers according to risk and are encouraged to partner with the federal government in developing strategies for moving from higher tiers with higher security costs to lower tiers with lower costs. Such an approach does not dictate what processes or technologies chemical plants can use but rather provides a strong incentive for investing in so-called inherently safer technologies or moving dangerous operations to more remote locations. Creating this incentive, however, will require that the DHS set standards for the physical protection of the most dangerous facilities that are more than just window dressing.

In this chapter, we provide background on the chemical industry, discuss why the industry's excellent record on safety does not translate into security, discuss previous attempts to legislate security measures, and conclude with a review of the Collins bill. Our ultimate recommendation is that the Collins bill should be modified to make the regulatory action stronger. Doing so would encourage industry members to take real steps toward reducing their vulnerabilities.

BACKGROUND

In the predawn hours of December 3, 1984, a tank holding methyl isocyanate at a Union Carbide plant in Bhopal, India, began to overheat. Water was introduced to the tank, causing a chemical reaction that within minutes raised the tank's internal temperature to over 200 degrees celsius. The heat generated a large volume of highly toxic gas, triggering release valves to prevent an explosion. The heavier-than-air gas rolled along the ground into the communities nearby the plant. In all, some 2,500 people were killed immediately, with ongoing health effects leading to an additional 15,000 deaths. The cause of the incident officially was considered to be a combination of poor maintenance practices, which led to the accidental introduction of water to the tank, and ineffective safety systems. Studies commissioned by Union Carbide, however, contend that the water was introduced through a direct connection to the tank by a malicious employee.²

Whether the Bhopal incident was due to poor maintenance or “damage by design,” there is little doubt that terrorists could reproduce similar results given the state of security at many chemical plants in this country. A reporter for the *Pittsburgh Tribune Review* has repeatedly infiltrated some of the most potentially dangerous chemical facilities in the nation. These include facilities operated by ACC members that adhere to the Responsible Care program. Security of facilities that store large quantities of chlorine, ammonia, and other hazardous chemicals was found to be lax. Problems included a lack of perimeter control and procedures to maintain entry-exit control at security gates.³ After the initial story ran, crews from *60 Minutes* were able to infiltrate the very same plants.⁴

The general consensus among the homeland security community is that the chemical industry remains vulnerable to a terrorist attack that could potentially kill thousands of Americans. The Brookings Institution in 2002 reported that an attack on toxic chemical plants ranks third, behind only biological and atomic attacks, in terms of possible fatalities.⁵ Much attention has focused on the worst-case scenario projections from facilities regulated by the Environmental Protection Agency (EPA), which predict many millions of fatalities in some instances. These estimates are likely overstated, however, since the EPA based its findings on crude models of chemical releases that do not take into account wind patterns and basic concepts of plume modeling. According to the Department of Homeland Security’s revised estimates, there are approximately 4,400 facilities that threaten 1,000 or more people each, with many facilities posing a threat to substantially more than that. In the event of a successful attack on a chemical facility, casualties could easily exceed the mark of just under three thousand who died on September 11. DHS planning scenarios leaked to the *New York Times* revealed that the department estimates that a detonation at a single chlorine plant could kill 17,500 people.⁶

Given the current low level of security and the potentially disastrous consequences of an attack, chemical facilities would be highly appealing targets for terrorists bent on mass slaughter. The DHS planning scenario postulates that a terrorist cell with a minimal technical knowledge of bomb-making, which is still easily found on the Internet, attacking a chemical facility storing toxic substances, could produce effects amplified exponentially beyond more conventional application of a simple bomb.

SAFETY AND SECURITY

Following the Bhopal incident, Congress amended the Clean Air Act Amendments (CAAA) to prevent a similar incident from occurring in the United States. The CAAA mandated that approximately 15,000 facilities develop and submit risk management plans (RMPs) to the EPA. RMPs are now required of any facility handling large quantities of any of 140 hazardous chemicals. Facilities that are required to submit RMPs must identify potential safety hazards and develop plans for reducing the risk of an unintentional release. These requirements have led to a successful partnership between the EPA and the chemical industry, resulting in an excellent record of safety.

Planning for safety, however, does not necessarily mean planning for security. Safety mechanisms are designed to protect against accidents. They may do little or nothing to prevent terrorists from causing an intentional release. The ACC and other industry associations have developed security standards for their respective members.

The ACC Responsible Care program started as a program aimed at improving environmental, health, and safety performance. Following the September 11 attacks, the ACC developed a security component for the program, the Responsible Care Security Code. The code requires ACC members to conduct facility security assessments and implement necessary improvements. One notable component of the code is that it requires the assessments and improvements to be audited by a third-party security firm. As impressive as the code sounds, the ACC consists of only 150 chemical companies and the code covers only a small percentage of chemical facilities. With no current federal mandate to track adoption of voluntary codes or audit adherence to these codes, it is unclear how effective such measures have been at increasing security.

The ACC has voiced support for varying legislative initiatives, while noting that competing companies that do not invest in security undercut ACC members that spend on security measures. Smaller chemical producers, on the other hand, maintain that security costs and compliance with security regulations will put them at a disadvantage against their larger competitors. If there is an attack, however, Congress is likely to quickly institute sweeping and ham-fisted security requirements for all chemical plants regardless of the voluntary measures adopted by some companies. The industry is therefore only as strong as its weakest link.

Such was the case after September 11, when the entire airline industry, not only American and United, was temporarily grounded and fear of flying threatened financial solvency across the industry. Smart security now may avoid the adoption of poorly and hastily thought out regulation following a successful attack.

INITIAL LEGISLATIVE RESPONSES

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, signed by President Bush in 2003, charges the EPA and DHS to work with Congress to develop legislation that requires “chemical facilities, particularly those that maintain large quantities of hazardous chemicals in close proximity to population centers, to undertake vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified.”⁷ Unfortunately, since the adoption of this strategy, no regulation has yet been promulgated.

In March 2003, the GAO recommended that the DHS and the EPA take a series of first steps, including the need to:

- ◆ identify high-risk facilities based on factors including the level of threat and collect information on industry security preparedness;
- ◆ specify the roles and responsibilities of each federal agency partnering with the chemical industry; and
- ◆ develop appropriate information-sharing mechanisms.⁸

Little of this legwork has been completed, mostly because the overall National Infrastructure Protection Plan (NIPP) that is meant to lay the framework for doing this in the chemical and other sectors has not been implemented.

Two relevant bills addressing chemical industry security received substantial consideration in the 108th Congress, but were not passed. The Chemical Facilities Security Act of 2003 (sponsored by Senator James Inhofe, R-OK) would have required chemical facilities to conduct vulnerability assessments, prepare and implement site security plans, and establish a timetable for reducing discovered vulnerabilities. The bill did not require facilities to submit their security plans to the Department of Homeland Security or any other federal agency.⁹ A competing bill, the

Chemical Security Act of 2003 (sponsored by Senator Jon Corzine, D-NJ), would have directed the EPA to designate high-priority chemical facilities based on the threat posed by an intentional release and require these facilities to conduct vulnerability assessments, identify hazards that would result from a release, and create a prevention, preparedness, and response plan. The Corzine bill also would have required facilities to share these assessments and plans with the EPA. The DHS and the EPA would jointly review the assessments and plans to determine compliance. The bill included a provision that required facilities to consider inherently safer technologies, for example, using less toxic chemicals.¹⁰ This provision was widely criticized for its vagueness and the potential to open the industry to micromanagement by federal officials.

Both bills focused on the category of facilities currently regulated under EPA's Risk Management Program requirements. However, these regulated facilities are only a portion of those of concern from a security perspective. Under the safety-oriented CAAA, facilities are able to avoid regulation by dividing large storage units of hazardous chemicals into smaller storage containers, thereby mitigating the potential damage caused by an accidental release. However, terrorists could cause a series of storage tanks to rupture and cause the same amount of damage as one large release. Hence, as an unintended consequence of a focus on safety, these facilities are operating under the radar of security efforts.¹¹

While a compromise bill made it through the Senate Environment and Public Works (EPW) Committee in October of 2003, action on it stalled on the Senate floor. Both the Inhofe and Corzine bills were pursued through the EPW Committee, but jurisdiction for the issue has since shifted to the Homeland Security and Governmental Affairs Committee, chaired by Senator Susan Collins (R-ME) and with ranking member Senator Joseph Lieberman (D-CT).

THE CHEMICAL FACILITY ANTI-TERRORISM ACT

This past December, Senator Collins introduced the Chemical Facility Anti-Terrorism Act of 2005. The bill addresses the issues that have kept past attempts to legislate from moving forward. It is largely consistent

with the general recommendations on how best to promote security in the private sector in Chapter 5. The Collins bill correctly treats most chemical facilities as high-impact targets, creates a regional approach to partnering with the industry, and uses a smart regulatory approach to produce better security. It is loosely modeled on the successful Maritime Transportation Security Act of 2002, which covers some chemical facilities located on or near the waterfront.

The bill would place chemical facilities into tiers grouped by risk, with higher tiers requiring higher levels of security. Within one year of enactment, the bill requires the DHS to set criteria determining which facilities are covered by the act, place facilities within tiers grouped by risk, and establish security standards for each tier. Facilities that are subject to the act would be required to conduct a vulnerability assessment, develop a security plan, and update their emergency response plans to take into account the consequences of intentional acts. The bill would grant the secretary of the DHS the authority to fine or close down facilities that are out of compliance. As discussed in Chapter 5, the bill calls for the creation of regional plans and regional offices to partner with the industry and conduct audits and inspections.

The tiered system does not explicitly require companies to consider so-called inherently safer technologies. It can, however, provide the impetus for companies to make such investments. The bill stipulates that companies can work with DHS to develop a plan for moving from a higher tier to a lower one. If the regulations promulgated for the higher-tiered facilities are appropriate, the costs of physical protection likely will be quite high. Over the long term, moving dangerous operations to more remote locations or investing in inherently safer technologies may be a prudent business decision in order for companies to avoid the costs of a higher-tier status. This is a strong example of how smart regulation can be used to promote security. Instead of Congress dictating the procedures that an industry must use, it can create a legal framework that encourages the industry members to make their own informed decisions on how to proceed. For this process to unfold, the regulations the DHS develops would have to be sufficiently strong.

Given the potential consequences of a successful attack on a high-risk facility, security standards should be similar to those for nuclear plants. Though there are problems that must be corrected in current nuclear facility security practices, as discussed in Chapters 8 and 14, the

approach used is certainly applicable to chemical facilities. Security at nuclear plants is developed according to a “design basis threat,” a profile of possible attack scenarios that plant security personnel must be able to manage. As at nuclear plants, security personnel guarding facilities in the highest-risk tier must have the legal authority to use deadly force to stop intruders. Without this capability, investments in fences, gates, and intrusion detection devices will prove little more than cosmetic security. For fences to be useful, they must be guarded by security personnel authorized to stop, with deadly force if necessary, anyone who tries to climb over them. This kind of authority is not to be taken lightly, but is ultimately necessary if physical security measures to prevent terrorists from striking these targets are to be effective.

Given the high cost of deploying such a security system, the relocation of plants or switching to safer materials might make sense. Moving from active security (requiring personnel to respond to an attack) to passive security (removing the vulnerabilities that make these facilities targets in the first place), should be the ultimate goal of a serious attempt to regulate security.

The Collins bill, like previous attempts to regulate chemical industry security, would require companies to conduct self-assessments that evaluate the vulnerability of the chemical plant. DHS would be required to develop standards for these assessments, and would have the legal authority to audit and conduct on-site inspections. Yet self-assessments are a weak basis on which to improve security. Reflecting our recommendations in Chapter 5, the bill should be amended to have DHS certify security professionals, and require companies to contract with these professionals to conduct the assessments. Such a model has worked well with the Securities and Exchange Commission in securities regulation, and also could work well with chemical industry security regulation.

Finally, the Collins bill includes a certification provision whereby companies found to be in compliance will be officially recognized by the Department of Homeland Security. This certification should come with a liability shield. Companies that have met their requirements under the law should not be sued if, despite the measures they have taken to improve security, they are successfully targeted by terrorists. In order to create an added financial incentive for investing in security, certification also should result in reduced premiums on terrorism insurance coverage.

RECOMMENDATIONS

The Chemical Facility Anti-Terrorism Act of 2005 has the potential to improve significantly the security of our nation's chemical facilities. Congress should move quickly to fix the problems we have outlined in the bill and then make it into law. These suggested changes include:

7.1. PROVIDING A STRONGER FRAMEWORK FOR DEVELOPING REGULATIONS THAT WILL FOCUS COMPANIES ON INVESTING IN PASSIVE SECURITY OVER ACTIVE SECURITY.

7.2. USING A "DESIGN BASIS THREAT" FOR DEVELOPING SECURITY REQUIREMENTS FOR FACILITIES IN THE HIGHEST-RISK TIER.

7.3. GIVING SECURITY PERSONNEL AT HIGH-RISK FACILITIES THE LEGAL AUTHORITY TO USE DEADLY FORCE AGAINST ATTACKERS.

7.4. ESTABLISHING A TRAINING AND CERTIFICATION PROGRAM UNDER WHICH SECURITY PROFESSIONALS CAN CONDUCT VULNERABILITY ASSESSMENTS AND ESTABLISH SECURITY PLANS.

7.5. PROVIDING LIABILITY PROTECTION AND TERRORISM INSURANCE PREMIUM REDUCTIONS FOR FACILITIES CERTIFIED AS BEING COMPLIANT.



In addition to these changes, Congress must provide sufficient funding to enforce the act. The proposed 2007 budget for the Department of Homeland Security includes a paltry \$10 million to establish an office to oversee chemical facility security. These funds are entirely insufficient and portend the elimination of the proposal for regional offices that will be crucial in partnering with the industry and in enforcing the provisions of the Collins bill.

