Order Code RL31530

Chemical Facility Security

Updated January 12, 2006

Linda-Jo Schierow
Specialist in Environmental Policy
Resources, Science, and Industry Division

Chemical Facility Security

Summary

Facilities handling large amounts of potentially hazardous chemicals (i.e., chemical facilities) might be of interest to terrorists, either as targets for direct attacks meant to release chemicals into the community or as a source of chemicals for use elsewhere. Because few terrorist attacks have been attempted against chemical facilities in the United States, the risk of death and injury in the near future is estimated to be low, relative to the likelihood of accidents at such facilities or attacks on other targets using conventional weapons. For any individual facility, the risk is very small, but the risks may be increasing — with potentially severe consequences for human health and the environment. Available evidence indicates that many chemical facilities may lack adequate safeguards.

Two federal laws require planning to protect the general public from accidental releases of hazardous chemicals, but neither law explicitly addresses terrorism. After 9/11, Congress enacted legislation that requires the Department of Homeland Security (DHS) to analyze vulnerabilities and suggest security enhancements for "critical infrastructure." The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188) and the Maritime Transportation Security Act (MTSA, P.L. 107-295) require vulnerability assessments and emergency response plans for some chemical facilities that supply drinking water or are located in ports, as well as security plans for chemical facilities in ports. Many other chemical facilities, including wastewater treatment facilities, remain unregulated.

Congress might choose to rely on existing efforts in the public and private sectors to improve chemical site security over time. Alternatively, Congress could expand existing environmental planning requirements for chemical facilities to require consideration of terrorism. DHS could be directed to oversee security enhancement at potentially dangerous facilities. Or, Congress might enact legislation to reduce risks, either by "hardening" defenses against terrorists (for example by increasing security patrols) or by requiring industries to consider use of safer chemicals, procedures, or processes. Restricting terrorists' access to information might be a least-cost approach to reducing risks, but it would also limit public access to information about potential risks and reduce accountability of facility owners. For more on this topic, see CRS Report RL33043, *Legislative Approaches to Chemical Facility Security*, by Dana A. Shea.

In the 109th Congress, two House bills and one Senate bill would require designated facilities to prepare vulnerability assessments and plans for increasing facility safety and security and for responding in the event of an emergency. H.R. 1562 and S. 2145 would require facilities to submit assessments and plans to DHS; under H.R. 2237, submissions would go to the Environmental Protection Agency (EPA). H.R. 2237 also would require consideration and use of "safer" technologies. S. 2145 would direct DHS to establish security performance standards for facilities, based on relative risk, and would allow facility owners to develop site-specific security measures to meet those standards. Other bills (S. 2052/H.R. 713 and S. 1995) aim to enhance security for agricultural businesses and wastewater treatment facilities. This report will be updated as warranted by congressional activity.

Contents

List of Tables

Chemical Facility Security

Introduction

The potential harm to public health and the environment from a large release of hazardous chemicals has long concerned the U.S. Congress. The sudden, accidental release in December 1984 of methyl isocyanate in an industrial incident at the Union Carbide plant in Bhopal, India, and the attendant loss of thousands of lives and widespread injuries spurred legislative proposals to reduce the risk of chemical accidents in the United States. For example, federal environmental laws were enacted in 1986 and 1990 to mitigate and reduce the risk of accidental releases of hazardous chemicals from manufacturing facilities, processing plants, and storage tanks. (These laws are discussed below.) The Hazardous Materials Transportation Act of 1975 was passed to protect the public and environment in the event of an accident during transportation of chemicals. Other federal laws coordinate preparedness planning and response to significant chemical spills (e.g., the Comprehensive Environmental Response, Compensation, and Liability Act).

The threat of terrorism manifested on September 11, 2001, prompted renewed congressional attention to the potential risks to public health and the environment posed by facilities handling large quantities of hazardous chemicals. Congress addressed chemical facility security when it enacted legislation establishing the Department of Homeland Security (DHS; P.L. 107-296). The law requires analysis of vulnerabilities and suggestions for security enhancements for "critical infrastructure." The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188) and the Maritime Transportation Security Act (MTSA, P.L. 107-295) require vulnerability assessments, security plans, and incident response plans for some chemical facilities which supply drinking water or are located in ports. Many other chemical facilities remain unregulated with respect to terrorism.[1] Thus, the 109th Congress is continuing to discuss the risks and consequences of potential terrorist attacks on chemical facilities and possible actions the federal government might take to prevent or reduce them.

This report provides background information and summarizes issues relevant to existing and proposed requirements aimed at reducing risks to the general public of exposure to hazardous chemicals as a result of terrorist acts at U.S. facilities where chemicals are produced, processed, stored, or used. It considers the likelihood and severity of harm that might result from terrorist attacks on chemical facilities, as well as from illicit use of such facilities to gain access to hazardous chemicals (or to precursor chemicals that can be used to produce hazardous chemicals). Federal requirements for contingency planning and responding to chemical emergencies after

---

[1] There is no universally accepted definition of "terrorism." Various definitions are discussed in CRS Issue Brief IB10119, *Terrorism and National Security: Issues and Trends*, by Raphael Perl.

they occur are not the focus of this report. In addition, it does not consider hazardous materials transport (or storage incidental to transport).

The report first describes the range of terrorist acts that might threaten chemical facilities and summarizes publicly available information relevant to risks: recent trends in terrorist activity, including chemical use by terrorists; expert estimates of the harm that might be inflicted through chemical terrorism; and assessments of the vulnerability of chemical facilities. The next section of the report discusses existing federal mandates and incentives for reducing risks of accidental releases from chemical facilities. The remainder of the report summarizes recent Administration and private sector initiatives to improve chemical site security; analyzes policy options and key issues; and describes legislation in the 109th Congress.

Risks of Terrorism at Chemical Facilities

Nature of Hazards. Potential terrorist acts against chemical facilities might be classified roughly into two categories: direct attacks on facilities or chemicals on site, or efforts to use business contacts, facilities, and materials (e.g., letterhead, telephones, computers, etc.) to gain access to potentially harmful materials. In either case, terrorists may be employees (saboteurs) or outsiders, acting alone or in collaboration with others. In the case of a direct attack, traditional or nontraditional weapons may be employed, including explosives, incendiary devices, firearms, airplanes, or computer programs.

In obtaining chemicals, a terrorist's intent may be to use them as weapons or to make weapons, including explosives, incendiaries, poisons, and caustics. Access to chemicals might be gained by physically entering a facility and stealing supplies, or by using legitimate or fraudulent credentials (e.g., company stationary, order forms, computers, telephones or other resources) to order, receive, or distribute chemicals.

Recent Trends in Overall Terrorist Activities. According to February 2003 testimony by the Director of the Federal Bureau of Investigation (FBI) to the U.S. Senate, there were 353 known or suspected acts of terrorism (including terrorist acts by Americans) perpetrated within the United States between 1980 and 2001.[2] Only a few incidents involved chemical facilities. Attacks during the 1990s claimed 182 lives and injured over 1,932 individuals.[3] In comparison, during the 1980s, although there were many more terrorist or suspected terrorist incidents, only 23 people were killed and 105 were injured.[4] Thus, although the total number of terrorist acts in the United States declined toward the end of the 20th century, the casualties due to terrorism increased.

---

[2] Mueller, Robert S., III, Director, Federal Bureau of Investigation. Testimony before the Senate Select Committee on Intelligence, Feb. 11, 2003, at [http://www.intelcenter.com/resource/2003/mueller.pdf], visited Feb. 4, 2005.

[3] The Oklahoma City bombing of the federal building in 1995 accounts for 168 of the 182 deaths during the decade.

[4] Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, Federal Bureau of Investigation, Department of Justice. *Terrorism in the United States 1999: 30 Years of Terrorism, A Special Retrospective Edition*, p. 16.

The same trends have been evident internationally, although there is considerable variation from year to year.[5] The year 2003 had 208 international terrorist attacks on noncombatants, a few more than 2002, but 42% fewer than in 2001.[6] There were 725 persons killed in 2002 and 625 persons (35 U.S. citizens) in 2003.[7]

In terms of U.S. casualties due to international terrorism, 2001 is the most costly year on record, with 2,689 people killed.[8] As noted by the FBI Executive Assistant Director for Counterterrorism and Counterintelligence, the attack of September 11, 2001, "marked a dramatic escalation in a trend toward more destructive terrorist attacks which began in the 1980s."[9]

> The September 11 attack also reflected a trend toward more indiscriminate targeting among international terrorists. The vast majority of the ... victims of the attack were civilians. In addition, the attack represented the first known case of suicide attacks carried out by international terrorists in the United States. The September 11 attack also marked the first successful act of international terrorism in the United States since the vehicle bombing of the World Trade Center in February 1993.[10]

Other potentially important trends identified by intelligence agencies include:

- an increase in activity by loosely affiliated extremists, both domestically and internationally; and
- the propensity of such groups to focus on producing mass casualties.[11] [12]

---

[5] The National Counterterrorism Center (NCTC) and the State Department changed the methodology for tabulating terrorist incidents in 2004, and ceased publication of *Patterns of Global Terrorism*. As a result, no comparable figures are available for 2004 or subsequent years. A database on terrorist incidents is maintained by the NCTC at [http://tkb.org/AboutTKB.jsp], visited Jan. 11, 2006.

[6] U.S. Department of State. 2004. *Patterns of Global Terrorism 2003*. Revised June 22, 2004. [http://www.state.gov/s/ct/rls/pgtrpt/2003/], visited Sept. 20, 2004.

[7] U.S. Department of State. 2004. *The Year in Review (Revised)*, at [http://www.state.gov/s/ct/rls/pgtrpt/2003/33771.htm], visited Sept. 20, 2004.

[8] Ibid., p. 180. The anthrax killings may or may not be found to meet the FBI definition of terror, depending on whether the criminal intended to further political or social objectives.

[9] Watson, Dale L., Executive Assistant Director, Counterterrorism and Counterintelligence, Federal Bureau of Investigation. Statement for the Record on the terrorist threat confronting the United States before the Senate Select Committee on Intelligence. Feb. 6, 2002. [http://www.fbi.gov/congress/congress02/watson020602.htm], visited Feb. 4, 2005.

[10] Ibid., p. 1.

[11] Ibid.

[12] Counterterrorism Division, Counterterrorism Threat Assessment and Warning Unit, Federal Bureau of Investigation, Department of Justice. *Terrorism in the United States 1999: 30 Years of Terrorism, A Special Retrospective Edition*, p. 25.

Trends in Chemical Terrorism. With respect to chemical and biological terrorism, hoaxes and unsuccessful attempts by terrorists to use chemicals increased throughout the 1990s. Loosely affiliated terrorist groups, in particular, have demonstrated a growing interest in chemical weapons and other weapons of mass destruction, but explosives are still the most frequently employed weapons.[13]

During the 1990s, both international and domestic terrorists attempted to use explosives to release chemicals from manufacturing and storage facilities. Most of these attempts were abroad in war zones such as Croatia, including attacks on a plant producing fertilizer, carbon black, and light fraction petroleum products; other plants producing pesticides; and a pharmaceutical factory using ammonia, chlorine, and other hazardous chemicals. All of these facilities were close to population centers. In the United States, there were at least two instances during the late 1990s when criminals attempted to cause releases of chemicals from facilities. One involved a large propane storage facility, and the other a gas refinery.[14]

Evidence that U.S. chemical facilities may be used by terrorists to gain access to chemicals also exists. For example, one of the 1993 World Trade Center bombers, Nidal Ayyad, became a naturalized U.S. citizen, graduated from Rutgers University, and worked as a chemical engineer at Allied Signal, from which he used company stationery to order chemical ingredients to make the bomb. According to a U.S. Prosecutor in the case against the bombers, though "some suppliers balked when the order came from outside official channels, when the delivery address was a storage park, or when [a co-conspirator] tried to pay for the chemicals in cash," others did not.[15] Moreover, testimony at the trial of the bombers indicated that they had successfully stolen cyanide from a chemical facility and were training to introduce it into the ventilation systems of office buildings.[16] More recently, chemical trade publications reportedly were found in al Qaeda hideaways.[17]

Predicted Risks of Chemical Terrorism. The validity of any risk assessment depends on how much is known about the hazard, risks (probabilities), adverse effects, events and conditions that lead to or modify adverse effects or risks, and populations or environments that influence or experience adverse effects. The most accurate, and therefore the most useful, risk assessments generally are for familiar, frequently occurring hazards and events with impacts that are experienced

---

[13] Ibid., pp. 17, 25.

[14] Department of Justice. *Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet*, Apr. 18, 2000. pp. 23-24.

[15] Parachini, John V. "The World Trade Center Bombers (1993)." In: Jonathan B. Tucker (ed.) 2000. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Cambridge, MA: MIT Press. p. 190. Citing the summation statement of Henry J. DePippo, Prosecutor, *United States of America v. Mohammad A. Salameh et al.*, S593CR.180 (KTD), Feb. 16, 1994, pp. 8435-8439.

[16] Ibid.

[17] Bond, Christopher. Statement on S. 2579. *Congressional Record*, Daily Edition, June 5, 2002, p. S5043.

with some regularity, such as severe storms or floods. In contrast, the risk of terrorist activity is unfamiliar (at least in the United States), rarely experienced, and likely to vary significantly over time, depending on rather unpredictable social and political phenomena.

The risk of terrorism targeting chemical facilities is particularly difficult to assess for at least three reasons:

- There are few prior examples of terrorists targeting chemical facilities;
- Numerous factors theoretically may increase or decrease risks; and
- Interactions among factors influencing risks are dynamic and changing.

In part, these difficulties stem from the nature of terrorism and the terrorists' deliberate efforts to do what is least expected — that is, to defy prediction. For these reasons, most experts have not tried to quantify risks; existing analyses of chemical terrorism risks in the open literature are speculative and qualitative.[18]

Until the mid to late 1990s, reports focused on the acquisition and use of chemical weapons, such as sarin or mustard gas. One of the most comprehensive of these reports was a 1995 review of the open literature on terrorism that was prepared for the Canadian Security Intelligence Service.[19] According to this review of the literature, "[t]hose authors who have speculated about the future terrorist use of chemical agents in particular have generally rated its likelihood as quite high."[20]

According to some, the risk also appears to be increasing. Many experts today believe that factors that might have inhibited proliferation and use of chemicals as weapons in the past are eroding. For example, some experts hypothesized several years ago that the combination of chemical and strategic skills necessary to create and deploy chemical weapons would prevent the lone terrorist from using them.[21] Security experts now believe that lack of personal expertise no longer limits chemical weapon use, because there is a tendency for terrorists with similar extreme views to affiliate loosely with others with complementary skills and abilities. Moreover, the rising level of education worldwide means that more people have the requisite

---

[18] Computerized databases on terrorist acts offer considerable promise for risk analysts who have access. Nevertheless, the unpredictable nature of individuals and of the social and political forces that shape them over time will continue to challenge predictions about future events.

[19] Purver, Ron. "Chemical and Biological Terrorism: the Threat According to the Open Literature." June 1995. Canadian Security Intelligence Service. [http://www.csis-scrs.gc.ca/eng/miscdocs/tabintr_e.html], visited Feb. 4, 2005.

[20] Ibid., Chemical Terrorism, p. 28. This prediction about the use of chemical agents contrasts with conventional wisdom that the probability of chemical weapon use is relatively small. The conventional prediction, however, focuses on military use of chemical weapons in future wars among nations, rather than on chemical use by terrorists.

[21] Ibid., p. 29.

training in chemical engineering, and the Internet has simplified communications, training, and cooperation within geographically dispersed terrorist groups.

Others have argued that chemical attacks would be unlikely, due to the difficulties of producing and effectively delivering chemical agents in sufficient amounts to produce mass casualties.[22] However, while this may be true with regard to military use on a large scale, where weapons are delivered by advanced systems, it is not necessarily relevant to terrorists who may have more limited ambitions. A 1999 report by the U.S. General Accounting Office (GAO, now the Government Accountability Office) summarized the situation —

> ... many conflicting statements have been made in public testimony before Congress ... concerning the ease or difficulty with which terrorists could effectively disseminate a chemical or biological agent on U.S. soil and cause mass casualties.[23]

GAO studied the threat and concluded that the ease or difficulty for terrorists to cause more than 1,000 casualties depends on the chemical or biological agent selected. The report stated —

> Experts from the scientific, intelligence, and law enforcement communities told us that terrorists do not need sophisticated knowledge or dissemination methods to use toxic industrial chemicals such as chlorine. In contrast, terrorists would need a relatively high degree of sophistication to successfully cause mass casualties with some other chemical and most biological agents.

On the other hand,

> "[t]errorists with less sophistication could make a chemical or biological weapon and disseminate agents, but these would be less likely to cause mass casualties."[24]

Other factors that might have inhibited chemical use by some terrorists in the past might not apply to loosely affiliated terrorist groups. For example, some experts argue that terrorists supported by nation-states have been reluctant to use chemical weapons for fear of offending other nations and neutral parties, particularly if the sponsors were signatories of the Chemical Weapons Convention.[25] Another possible deterrent to chemical use, fear of retaliation, probably is of little concern to attackers with no identifiable homeland or headquarters. Lack of a homeland might also lessen concern about environmental damage that may be associated with chemical production. Finally, one must presume that occupational safety would be of limited

---

[22] Purver, p. 5-13.

[23] U.S. GAO. *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks.* Sept. 1999. GAO/NSIAD-99-163. Washington, DC: U.S. Govt. Print. Off. p. 1.

[24] Ibid., p. 3.

[25] Purver, p. 28.

concern to terrorists who are not accountable to a government, and who are willing to sacrifice their own lives for a religious, political, or social cause.

However, many experts believe that the relative risk of terrorism involving chemical weapons remains small. This point was stressed by John V. Parachini, a senior associate at the Center for Nonproliferation Studies, Monterey Institute of International Studies at a 1999 hearing before the U.S. House of Representatives, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations. Referring to the risk of any use of chemical or biological weapons he stated:

> ... attacks with chemical and biological weapons are strikingly infrequent and the number of fatalities and casualties are far lower than those caused by conventional explosives. According to an analysis of 105 U.S. incidents featured in the Monterey Institute database from 1900 to 1998, only one fatality resulted from a [chemical or biological weapon] attack. This incident involved a 1973 assassination of an Oakland, California school superintendent by the Symbionese Liberation Army.[26]

Severity of Harm. It is generally agreed that chemical agents are likely to be the least lethal of the three "weapons of mass destruction." In part, this judgment reflects the difficulty of producing and delivering large quantities of a lethal chemical to the target area prior to release. On the other hand, industrial chemicals and pesticides are readily available for purchase, and are stored in large quantities in thousands of locations throughout the United States, often near population centers. A key question for chemical facilities then is "How much damage could terrorists do using existing stationary chemical manufacturing, processing, distribution, and storage facilities?"

There are two key sources of information for answering this question: accident reports and hazard assessments conducted by facility personnel or outside experts. There is no comprehensive database for either kind of information,[27] but various groups have used publicly available data to estimate hazard potential, usually limited to accidental releases of chemicals from chemical facilities.

A 1998 report by the U.S. Public Interest Research Group (US PIRG) and the National Environmental Law Center, *Too Close to Home: Chemical Accident Risks in the United States*, addressed the distribution of chemical facilities in the United States relative to population distribution. It stated that "more than 41 million Americans live within range of a toxic cloud that could result from a chemical

---

[26] U.S. Congress. House Committee on Government Reform. Subcommittee on National Security, Veterans' Affairs, and International Relations. *Combating Terrorism: Assessing the Threat*. Hearings, 106th Cong., 1st sess., Oct. 20, 1999. Washington, U.S. Govt. Print. Off., 2000, pp. 55-56.

[27] The most comprehensive, but still incomplete, listing of chemical spills and releases is kept by the National Response Center and available on the Internet at [http://www.nrc.uscg.mil/foia.html], visited Feb. 4, 2005.

accident at a facility located in their home zip code."[28] Those 41 million Americans live in zip codes that contain manufacturing companies with "vulnerable zones" extending more than three miles from the facility, the report states. A "vulnerable zone" is the geographic area that could be affected by the worst possible accident at a facility.[29] According to the report, the estimate of 41 million Americans at risk may underestimate the hazard, because it was based on "assumptions about facility and atmospheric conditions that would lead to small vulnerability zones."[30] To produce the estimate, the study author stated that he used standard methodology used by the U.S. Environmental Protection Agency (EPA) and data on chemical storage from EPA's 1995 Toxics Release Inventory, a database of routine releases of industrial chemicals from manufacturing facilities.

Hazard estimates by James C. Belke, an EPA employee in the Chemical Emergency Preparedness and Prevention Office, are more detailed. Based on a preliminary analysis of approximately 15,000 facility risk management plans for chemical facilities that were filed under the Clean Air Act, Section 112(r) before September 25, 2000,[31] Belke concluded that the median distance from a facility to the outer edge of its vulnerable zone is 1.6 miles in the case of toxic worst case scenarios, and 0.4 miles for flammable worst case scenarios. However, many facilities reported vulnerable zones potentially extending 14 miles from the facility (primarily for releases in urban areas of chlorine stored in 90-ton rail tank cars) and 25 miles (for releases in rural terrain of chlorine stored in 90-ton rail tank cars). Other chemicals for which reported vulnerable zones equaled or exceeded 25 miles include anhydrous ammonia, hydrogen fluoride, sulfur dioxide, chlorine dioxide, oleum (fuming sulfuric acid), sulfur trioxide, hydrogen chloride, hydrocyanic acid, phosgene, propionitrile, bromine, and acrylonitrile.)

Belke found the median population "affected" in a worst case accident was 15 people, for a flammable substance, while the median for toxic substances was 1,500 people.[32] ("Affected" means potentially exposed. It is highly unlikely that all people within the vulnerable zone would be exposed due to a single release. However, anyone within the zone could be in the path of the chemical released, given certain environmental conditions.) Further EPA analysis of risk management plans submitted by facilities handling chemicals covered by the CAA Section 112 revealed that at least 123 plants reported a worst-case scenario with a vulnerability zone

---

[28] Laplante, Allison. 1998. *Too Close To Home: A Report on Chemical Accident Risks in the United States*. U.S. Public Interest Research Group. [http://uspirg.org/uspirg.asp?id2=5067&id3=USPIRG&], visited Jan. 11, 2006.

[29] "Vulnerable zones" apply to facilities required to prepare risk management plans under the Clean Air Act, Section 112(r). By definition, people within the zone could (but would not necessarily) sustain serious injuries from short-term exposures.

[30] Laplante, Executive Summary. p. 2.

[31] Belke, James C. "Chemical Accident Risks in U.S. Industry — a Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities," Sept. 25, 2000, p. 24, at [http://www.epa.gov/swercepp/pubs/stockholmpaper.pdf], visited Jan. 11, 2006.

[32] Belke, p. 26.

containing more than a million people.[33] The analysis also found that more than 700 plants could threaten 100,000 people, and at least 3,000 facilities could threaten 10,000 people in the vicinity.[34]

The Department of Justice (DOJ) analyzed EPA data and concluded that among facilities submitting risk management plans to EPA, more than 7,000 facilities projected worst case scenarios for toxic substances that could potentially affect more than 1,000 people.[35] Almost 1,700 facilities reported the possibility that a less extreme accident might potentially affect more than 1,000 people.[36]

Histories of actual accidents (as opposed to hypothetical worst-case scenarios) for facilities submitting risk management plans to EPA prior to October 21, 1999, were summarized in a working paper prepared by the Center for Risk Management and Decision Processes at the Wharton School, University of Pennsylvania.[37] Of 14,500 reporting facilities, 1,145 reported 1,913 accidents between June 21, 1994 and June 20, 1999. Of the 1,145 facilities reporting accidents, 346 facilities had multiple accidents. Half of the chemicals for which risk management planning is required under the CAA Section 112(r) were involved in accidents. Half of the accidents resulted in reported injuries to workers. Accidents caused a reported 1,897 injuries and 33 deaths to employees, 141 injuries and no deaths to non-employees. No deaths were reported off-site. However, over 200,000 community residents were involved in evacuations and shelter-in-place incidents.[38]

Further analysis by the Wharton group revealed that the risk of accidental chemical releases and of worker injuries or property damage increased with the size

---

[33] Belke, J. (2001), "Chemical Accident Risks in U.S. Industry — A Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities," Proceedings of the 10th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Stockholm, Sweden, Pasman, Fredholm, and Jacobson (eds.), Elsevier Science B.V. — Note: This does not mean that more than a million people would be exposed and injured, but rather that, depending on wind direction and other factors, some portion of the population in the zone might be exposed and injured.

[34] Ibid. These numbers change each month, as facilities open or close, or change production processes and chemical quantities. As of June 1, 2005, EPA has approximately 13,260 facilities registered which project potential off-site consequences to one or more community residents in the event of a worst-case chemical release. Of these, roughly 600 facilities report vulnerability zones encompassing populations of more than 100,000, and about 2,200 facilities potentially threaten some portion of populations ranging between 10,000 and 99,999 residents. More than 1,000 RMP facilities report worst-case off-site consequence scenarios that threaten no residents.

[35] Department of Justice, p. 13.

[36] Ibid.

[37] Kleindorfer, Paul R., Harold Feldman, and Robert A. Lowe. "Accident Epidemiology and the U.S. Chemical Industry: Preliminary Results from RMP*Info." Working Paper 00-01-15. Center for Risk Management and Decision Processes, The Wharton School, University of Pennsylvania. Revised March 6, 2000. 27 p.

[38] Ibid., p. 9.

of the facility (from 10 to 1,000 full-time equivalent employees or FTEs).[39] Note that this refers to accidents of any kind, not to worst-case events. In addition, facilities reporting that they handled large amounts and many types of chemicals had much higher accident rates than facilities handling smaller amounts and fewer types of chemicals. The probability that a facility had experienced a chemical accident of any size approached 100% for the very largest chemical manufacturers. Toxic chemicals were more strongly associated with worker injuries, while flammable chemicals were more strongly associated with property damage. No regional trends in accident rates were discovered (i.e., facilities in various geographical regions had similar accident rates).

Risk management plans submitted to the EPA report the worst-case potentially affected population for a release from a single process. As such, these populations may under-represent the population potentially affected as a consequence of a terrorist attack. Approximately 70% of RMP facilities possess reportable quantities of chemicals in amounts greater than a single process. For roughly 10% of RMP facilities, the quantity of chemical on-site is more than 10 times the quantity in the single process used to calculate the worst-case scenario. Some 250 facilities report having 100 times as much chemical on-site as is found in the single process. Thus, the EPA methodology for calculating the potentially affected population in the worst case, which was developed for accidental releases, may understate the potential worst-case consequences of a terrorist attack.

In contrast to the above figures, which all were based on hypothetical or actual accidents described in risk management plans, the *Washington Post* reported March 12, 2002, that a classified study conducted by the U.S. Army Surgeon General dated October 29, 2001, found that a terrorist attack resulting in a chemical release in a densely populated area could injure or kill as many as 2.4 million people.[40] According to the news article, the study found "even middle-range casualty estimates from a chemical weapons attack or explosion of a toxic chemical manufacturing plant are as high as 903,400 people."[41] The worst-case estimate of 2.4 million casualties from a chemical release was roughly half the surgeon general's estimate for casualties due to widespread use of biological weapons, according to the report. The Army Surgeon General recently explained that the estimate of 2.4 million casualties is of "the number of people who might request medical treatment during a total release of a large industrial chemical manufacturing plant, in a densely populated area, and under ideal weather conditions for maximum exposure."[42] As in most

---

[39] Elliott, Michael R., Paul Kleindorfer, and Robert A. Lowe. "The Role of Hazardousness and Regulatory Practice in the Accidental Release of Chemicals at US Industrial Facilities." Working Paper 01-37-PK. Risk Management and Decision Processes Center, The Wharton School, University of Pennsylvania. Summer 2001. 22 p. [http://opim.wharton.upenn.edu/risk/downloads/01-37-PK.pdf], visited Jan. 11, 2006.

[40] Pianin, Eric. "Study Assesses Risk of Attack on Chemical Plant." *Washington Post*, Mar. 12, 2002. p. A8.

[41] Ibid.

[42] "Army Recants Attack Estimates." *Chemical Week*, May 22, 2002. p. 38.

studies of this kind, some question the magnitude and likelihood of the casualty estimates.

In 2004, the Department of Homeland Security used EPA data to estimate the number of potential fatalities that might result if *all* the various chemicals at a facility were released suddenly.[43] The purpose of the exercise was to allow DHS to prioritize chemical facility sites for inspections. Assuming that released chemicals would move in the direction of the prevailing winds, DHS determined possible fatalities within a wedge-shaped zone. It identified two facilities that threaten at least one million people downwind. DHS selected 360 facilities for its attention in the near term based on these estimates.

In July 2004, the Homeland Security Council issued 15 national planning scenarios to guide federal, state, and local homeland security preparedness activities.[44] Included in these scenarios are two that refer to industrial chemical releases. One describes a terrorist assault on a petroleum refinery while the other treats the release of a large volume of chlorine from an industrial facility. The planning figures cited for the hypothetical refinery attack include 350 fatalities and an additional 1,000 casualties. For the chlorine release, 17,500 fatalities, 10,000 severe injuries, and 100,000 additional casualties are postulated.

More recent calculations by DHS, based on more sophisticated models, have reduced hazard estimates.

> In our best estimate, based on an incredible amount of modeling that we've done, the highest-risk facility in the United States would produce under 10,000 potential fatalities and less than 40,000 people that would demonstrate some effects in terms of anywhere from a near-death experience from exposure to inhalation of the toxic chemical to a minor skin blemish caused by irritation through contact with the chemical.[45]

Chemical Site Vulnerability. CRS identified two publicly available reports that assess site security at U.S. chemical plants. In addition, investigative reports published in newspapers or documented with video recordings indicate that reporters have been able to visit various facilities without being supervised. The studies and selected newspaper accounts are summarized below.

Prior to September 11, an assessment of chemical plant site security by the Agency for Toxic Substances and Disease Registry (ATSDR) was considered by

---

[43] Block, Robert. "Chemical Plants Still Have Few Terror Controls." *Wall Street Journal*. Aug. 20, 2004, p. B1.

[44] Homeland Security Council, The White House, National Planning Scenarios — Executive Summaries, July 2004. [http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04.htm], visited July 29, 2005.

[45] Stephan, Robert. Testimony before the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Homeland Security Committee, June 15, 2005.

many to be the most comprehensive analysis that was publicly available. ATSDR researchers reviewed national statistics on domestic terrorism compiled by the FBI in 1995, and interviewed security staff from facilities and potential targets in one community with numerous chemical plants.[46] ATSDR researchers concluded:

- "security at chemical plants ranged from fair to very poor;"[47]
- chemical plant security managers "were very pessimistic about their ability to deter sabotage by employees, yet none of them had implemented simple background checks for key employees such as chemical process operators"; and
- "none of the corporate security staff had been trained to identify combinations of common chemicals at their facilities that could be used as improvised explosives and incendiaries."[48]

The full ATSDR report was never made public, but a DOJ report noted that

> ... among the 'soft targets' that the ATSDR identified as potential terrorist sites were chemical manufacturing plants (chlorine, peroxides, other industrial gases, plastics, and pesticides); compressed gases in tanks, pipelines, and pumping stations; and pesticide manufacturing and supply distributors.[49]

The DOJ released a study April 18, 2000, describing the risk of terrorism aimed at chemical plants.[50] It concluded that "the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible."[51] The study also noted that security at many industrial facilities generally is "not as substantial as the security at other comparable potential terrorist targets."[52]

In April and May, 2002, six to seven months after September 11, 2001, the *Pittsburgh Tribune-Review* published a series of articles describing an investigation of plant security conducted by the paper's reporters. On April 7, 2002, the newspaper stated that "anyone has unfettered access to more than two dozen potentially

---

[46] ATSDR. Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention. At [http://www.mipt.org/pdf/industrialchemicalsandterrorism.pdf].

[47] Greenpeace activists dramatized the poor security at one chlorine manufacturing plant in Feb. 2001. According to a report in the *Washington Post*, activists scaled the fence of a large Dow Chemical plant near Baton Rouge, Louisiana, and gained access to the control panel that regulates discharges into the Mississippi River. ("Toxic Chemicals' Security Worries Officials." *Washington Post*, Nov. 12, 2001, p. A14.)

[48] ATSDR studied two communities in different parts of the United States but only interviewed plant security personnel in one community.

[49] Department of Justice, p. 27.

[50] Ibid.

[51] Ibid., p. 2.

[52] Ibid., p. 30.

dangerous plants in the region" (referring to western Pennsylvania).[53] The author of the report continued:

> The security was so lax at 30 sites that in broad daylight a Trib reporter — wearing a press pass and carrying a camera — could walk or drive right up to tanks, pipes and control rooms considered key targets for terrorists.

The report was based on reporters' trips to 30 plants in western Pennsylvania which have filed risk management plans under the Clean Air Act, Section 112. Two of the plants were among the 123 plants nationwide that projected potential risks to more than 1,000,000 residents in the event of a worst-case accident or attack.[54] The 30 companies constituted more than half of the 61 sites in the region required to file risk management plans. Fifteen of the sites to which reporters gained unchallenged access were water treatment facilities in Pennsylvania and Maryland.

In May, another *Tribune-Review* article described a similar investigation of 30 additional plants in Houston, Baltimore, and Chicago.[55] The report concluded that security was lax at some of "the potentially deadliest plants" in all three cities; access was easy to some sites owned by corporations with large security budgets; employees, customers, neighbors, and contractors "not only let a stranger walk through warehouses, factories, tank houses and rail depots, but also gave directions to the most sensitive valves and control rooms"; and access to 19 sites was allowed due to "unguarded rail lines and drainage ditches, dilapidated or nonexistent fences, open doors, poorly angled cameras and unmanned train gates."

Chemical manufacturers and users contacted by reporters said that they had bolstered security recently. Several site managers reported that they made immediate changes in procedures or construction plans in response to security breaches by the reporters. But security cannot be ensured "overnight,"according to the president of the Pennsylvania Chemical Industry Council,[56] and it can be expensive. For example, the newspaper reported that U.S. Steel spends more than $1 million each year to equip, train, and hire its own hazardous chemicals response team, firefighters, paramedics, and gate guards at its coke factory.[57] The American Chemistry Council, which represents large chemical manufacturers, has reported that since September 11,

---

[53] Prine, Carl. "Lax Security Exposes Lethal Chemical Supplies." *Pittsburgh Tribune-Review*, Apr. 7, 2002, at [http://www.pittsburghlive.com/x/tribunereview/specialreports/potentialfordisaster/s_64612.html], visited Jan. 11, 2006.

[54] As noted above, these numbers change each month, as facilities open or close, or change production processes and chemical quantities. As of June 1, 2005, EPA had approximately 110 facilities registered which projected potential off-site consequences to a million or more community residents in the event of a worst-case chemical release.

[55] Prine, Carl. "Chemicals Pose Risks Nationwide." *Pittsburgh Tribune-Review*, May 5, 2002.
[http://www.pittsburghlive.com/x/tribune-review/specialreports/potentialfordisaster/s_69664.html], visited Jan. 11, 2006.

[56] Prine, Apr. 7, 2002.

[57] Ibid.

2001, its members have spent over $2 billion at about 2,000 facilities (about $1,000,000, on average, per facility).[58]

Television crews again entered and photographed chemical storage areas in November 2003.[59] Robert Full, Chief of the Allegheny County Department of Emergency Services in Pennsylvania testified February 23, 2004, before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, that there continued to be facilities in his county "that one could walk straight in under the guise of darkness and cause significant damage and public danger." He stated, "Some of the facilities have no more security than maybe perhaps a padlock or a chain."

In mid-2004, surveys were distributed to 189 U.S. chemical facilities where workers were represented by the Paper, Allied-Industrial, Chemical and Energy Workers International Union (PACE). Of the 133 surveys returned, 125 were from facilities where workers agreed that there were quantities of hazardous materials on site large enough to cause a catastrophic event if they were released. Responses to the survey indicated that surveyed workers believed nearly three-quarters of the plants had improved systems to guard toxic chemicals and had conducted drills to respond to an intrusion by terrorists.[60] On the other hand, according to employees who responded to questionnaires, fewer than half had improved communications, emergency response training, warning signals, or protective equipment, or contacted local first responders about the hazards on their sites. Nearly two-thirds of the plants had not discussed terrorist concerns with neighbors, according to surveyed workers.[61]

Conclusion. Whether recent trends in domestic and international terrorism will continue into the future, and whether they will be reflected in risks to U.S. chemical facilities, is unknown. Historically, there have been very few terrorist attacks on chemical facilities in the United States. Therefore, the estimated risk of death and injury from such attacks in the immediate future is low relative to the likelihood of other hazardous events, such as industrial accidents or terrorist attacks on other targets using conventional weapons. For any individual chemical plant, the

---

[58] American Chemistry Council. News & Media website. Security. At [http://www.accnewsmedia.com/site/page.asp?TRACKID=&VID=1&CID=361&DID=1313&PSID=ACC], visited July 9, 2005.

[59] CBS News. "U.S. Plants: Open to Terrorists." Sixty Minutes. Nov. 17, 2003. At [http://www.cbsnews.com/stories/2003/11/13/60minutes/main583528.shtml], visited Jan. 11, 2006.

[60] New Perspectives Consulting Group, Inc., PACE Evaluation Team. October 2004. *PACE International Union Survey: Workplace Incident Prevention and Response Since 9/11 Report. Durham, NC.* p. 48.

[61] The 125 facilities where surveys were distributed were subject to risk management planning requirements of the Clean Air Act, Section 112(r), based on public databases that were available and current in 2002. Therefore, the survey in 2004 may have included a few facilities that were no longer covered by RMP requirements. Also, the PACE report notes in the Executive Summary on page iii, "This survey looked at perceptions only. It did not include an independent assessment of, for example, which employees actually received training since September 11, 2001, or which actions companies actually took."

risk of attack is extremely small. However, the overall risks to chemical facilities may be increasing.

In contrast to the low probability of chemical terrorism, possible consequences for human health and the environment from such an event could be severe. Moreover, limited evidence suggests that chemical facilities may be "soft targets," lacking in adequate safeguards against criminal and terrorist attacks.

Federal Requirements Established Prior to September 11, 2001, To Reduce Risks at Chemical Facilities

Two key federal laws require or encourage certain chemical facility operators to reduce risks to the general public associated with releases of hazardous chemicals: the Emergency Response and Community Right-to-Know Act (EPCRA) and the Clean Air Act (CAA). Both focus on accidental releases of hazardous chemicals.

EPCRA. In 1986, two years after the Bhopal accident, Congress enacted EPCRA (codified at 42 U.S.C. 11001-11050) as Title III of the Superfund Amendments and Reauthorization Act (P.L. 99-499).[62] EPCRA mandated the establishment of State Emergency Response Commissions (SERCs) and Local Emergency Response Committees (LEPCs) to coordinate planning and response to potentially large releases of specified "extremely hazardous substances."[63] The act requires facility operators, LEPCs, and SERCs to prepare contingency plans for such releases.

Facility managers are required to provide information to LEPCs and local emergency responders (fire fighters, police officers, etc.) about chemicals present at facilities and to notify those officials in the event of a sudden release. EPCRA requires local officials to provide information about emergency plans and chemical hazards to the general public.

EPCRA's reporting and disclosure requirements are meant to facilitate planning, but sometimes they also promote risk reduction. For example, facility managers concerned about community relations sometimes reduce use of particularly toxic or otherwise hazardous materials, sometimes to the point that they no longer have to report, because they no longer handle reportable quantities of EPCRA chemicals. In

---

[62] For additional information about EPCRA, see CRS Report RL30798, *Environmental Laws: Summaries of Statutes Administered by the Environmental Protection Agency*, by Susan Fletcher, coordinator.

[63] EPCRA required EPA to list "extremely hazardous substances" and to establish threshold planning quantities for each substance. Originally, Congress defined chemicals as "extremely hazardous substances" if they appeared on a list EPA published in Nov. 1985 as Appendix A in "Chemical Emergency Preparedness Program Interim Guidance." However, Congress gave EPA authority to revise the list and the threshold quantities of chemicals. Based on listing criteria, the intent appears to be to include only chemicals in quantities that could harm people exposed to them for only a short period of time. Currently, there are approximately 356 such substances listed. For the list, see [http://www.epa.gov/swercepp/ehs/ehsalpha.html], visited Jan. 11, 2006.

other cases, the public disclosure requirement may encourage them to change chemical processes and handling in order to reduce the risk of reportable spills.

Although EPCRA requires facility reporting and cooperation in local emergency response planning, and it may encourage risk reduction, it stops short of requiring facilities to assess or reduce risks of chemical releases.[64] Instead, the act directed the EPA to study the problem and to identify any gaps in federal regulation.

CAA Section 112(r). In 1990, data accumulated by EPA on chemical accidents in the United States prompted Congress again to address the threat of catastrophic releases of chemicals that might cause immediate deaths or injuries in communities. It amended the Clean Air Act (CAA) to mandate EPA oversight of risk management planning at facilities that handle more than specified threshold quantities of hazardous substances.[65] The act defined "hazardous substances" to include chlorine, anhydrous ammonia, methyl chloride, ethylene oxide, vinyl chloride, methyl isocyanate, hydrogen cyanide, ammonia, hydrogen sulfide, toluene diisocyanate, phosgene, bromine, anhydrous sulfur dioxide, sulfur trioxide, and at least 100 other chemicals to be designated by EPA. EPA was directed to designate chemicals posing the greatest risks to human health or to the environment, based on three criteria: severity of potential acute adverse health effects, the likelihood of accidental releases, and the potential magnitude of human exposure. EPA promulgated a list of 77 acutely toxic substances, 63 flammable gases and volatile flammable liquids, and "high explosive substances" (59 *Federal Register* 4478, January 31, 1994). Fourteen chemicals met EPA criteria for listing as both toxic and flammable substances. The list was amended several times, notably on January 6, 1998 (63 *Federal Register* 640-645) to exclude explosive substances, and on March 13, 2000 (65 *Federal Register* 13243-13250) to exclude flammable substances when used as a fuel, or held for sale as a fuel at a retail facility. Selected categories of industries with large numbers of reporting facilities are identified in **Table 1**.

The CAA Section 112(r) imposes "a general duty" on owners and operators of facilities producing, processing, handling or storing any "extremely hazardous substance" to detect and prevent or minimize accidental releases and to provide prompt emergency response to a release in order to protect human health and the environment. The act requires owners and operators of covered facilities to prepare Risk Management Plans (RMPs) that summarize the potential threat of sudden, large releases of certain chemicals, including the results of off-site consequence analysis (OCA) for a worst-case chemical accident, and facilities' plans to prevent releases

---

[64] Many proponents of the reporting provisions of EPCRA argue, however, that public disclosure of information about chemicals present and released into communities sometimes prompts facility operators to reduce risks.

[65] The Clean Air Act Amendments of 1990 gave responsibility for the prevention of accidental chemical releases to the Occupational Safety and Health Administration (OSHA) and EPA. OSHA has responsibility for the protection of workers from accidental chemical releases and has promulgated the Process Safety Management Standard (29 CFR 1910.119) in response to this requirement. EPA has incorporated the OSHA Process Safety Management Standard as the chemical accident prevention program for certain facilities subject to both rules.

and mitigate any damage. Plans were to be submitted to EPA and made "available to the public" by June 21, 1999. EPA is required to review RMPs regularly, and if necessary, require revisions. EPA has delegated this responsibility to some states and localities.[66] (All states have authority to review RMPs at facilities that are major sources of air pollution, which are required to obtain permits under Title V of the Clean Air Act.) Plans must be revised and resubmitted to EPA every five years. Many facilities were required to submit updates by the end of June 2004.

In October 1996, the Accident Prevention Subcommittee of the Clean Air Act Advisory Committee to EPA created the Electronic Submission Workgroup to consider the technical and practical issues associated with an electronic database of risk management plans. In spring 1997, the workgroup unanimously agreed that EPA should provide full, unrestricted access via the Internet to most RMP information. However, advisors did not reach consensus regarding access to OCA data.

There were concerns that in facilitating electronic access to the general U.S. public through the Internet, EPA also would be facilitating access to these data internationally, which might permit misuse by terrorists.[67] Several members of the Accident Prevention Subcommittee recommended EPA undertake a security study to determine how much risk might increase as a result of putting OCA data on the Internet. Aegis Research Corporation, ICF Incorporated, and Science Applications International Corporation conducted the security study for EPA. The Agency concluded from the study that —

> ... the risk (although still very small) was slightly more than two times higher with unrestricted availability of the RMP with OCA data on the Internet. This increase reflects several factors, including the nature of the OCA data elements and the enhanced accessibility of data on the Internet to an international audience. Taken together, the primary utility of the unrestricted RMP and OCA data to a terrorist emerges from the capability to scan across the entire country for the "best" targets.[68]

---

[66] EPA has delegated authority to implement CAA Section 112(r) to the following states, territories, and localities: Delaware, Florida, Georgia, Kentucky, Mississippi, New Jersey, North Carolina, Ohio, South Carolina, Puerto Rico, Virgin Islands, Jefferson County, Kentucky, Buncombe County and the City of Asheville, North Carolina, Forsyth County, North Carolina, and Allegheny County, Pennsylvania. Rhode Island, Nevada, and Hawaii are seeking delegated authority. See [http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/112r-sts.htm#StateDelegation], visited Feb. 10, 2005.

[67] U.S. EPA. *Security Study: An Analysis of the Terrorist Risk Associated with the Public Availability of Offsite Consequence Analysis Data under EPA's Risk Management Program Regulations*. EPA 550-R97-003. Dec. 1997. p. 1.

[68] Ibid., p. 10.

Table 1. Number of Facilities Reporting Risk Management Plans to EPA in Selected Industrial Categories

Industrial Categories (NAICS code)[a]	Number of registered facilities (Total = 14,343)
Farm supplies wholesalers (42291, 42491)	3,699
Water supply and irrigation (22131)	1,777
Wastewater treatment (22132)	1,157
Refrigerated warehousing and storage facilities (49312)	717
Support activities for crop production (11511)	439
Oil and gas extraction (21111)	495
Meat processing (31161)	460
Other chemical and allied production wholesalers (42269,42469)	447
Basic organic chemical manufacturing (32519)	357
Electric power generation (22111)	322
Basic inorganic chemical manufacture (32518)	319
Farm production warehousing and storage (49313)	307
Plastics material and resin manufacturing (32521)	283
Fertilizer manufacturing (32531)	224
Other Farm Product Raw Material Merchant Wholesalers (42459)	179
Petroleum refineries (32411)	153
Petroleum bulk stations and terminals (42271, 42471)	142
All other chemical product manufacturing (32599)	133
Industrial gas manufacturing (32512)	130
Corn farming (111150)	116
General warehousing and storage facilities (49311)	102
Other	2,385

Source: Congressional Research Service. Numbers were obtained by searching the risk management plans for U.S. facilities using the June 1, 2005 version of the EPA National Database (with off-site consequence data) and EPA's software RMP*Review (version 3.1). Facilities that have deregistered are not included in the tallies.

a. North American Industry Classification System (NAICS) codes.

In December 1997, EPA began discussions with the FBI and other federal agencies about the electronic RMP distribution plan. National security concerns centered on the OCA data and their potential utility to terrorists. An interagency agreement was reached in late October 1998 that OCA data would not be included in RMP information placed on the Internet. Instead, EPA would make "appropriate" OCA data available in some form on request, but access would be restricted and not anonymous.[69] The possibility that OCA data could have been distributed via the Internet remained, however, because it could have been obtained and distributed by any citizen under the Freedom of Information Act (FOIA), according to the EPA Legal Counsel.

To address the security concerns raised by the Section 112(r) requirements, the Clinton Administration submitted draft legislation to Congress May 7, 1999. Congress enacted an amended version of the legislation as an amendment to S. 880, the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (P.L. 106-40). The new law amended Section 112 of the CAA to exempt OCA data from disclosure under FOIA, and limited public availability until EPA and DOJ issued regulations in August, 2000.

The final RMP regulation on data access was published August 4, 2000.[70] It allows public access to paper copies of sensitive OCA information through federal reading rooms, approximately one per state,[71] and provides Internet access to the OCA data elements that pose the least serious criminal risk. State and local agencies are encouraged to provide the public with read-only access to OCA information on local facilities. At the federal reading rooms, members of the public may read OCA information for up to 10 facilities per calendar month and for all facilities with potential effects in the jurisdiction of the local emergency planning committee. State and local officials and other members of the public may share OCA information as long as the data are not conveyed in the format of sensitive portions of the RMP or any electronic database developed by EPA from those sections.[72] A Clinton Administration proposal to implement the final rule (66 *Federal Register* 4021, January 17, 2001) would have allowed people to view plans of facilities outside their local area and enhanced access for "qualified researchers." The draft plan was rescinded by the Bush Administration (66 *Federal Register* 15254, March 16, 2001).

---

[69] Blitzer, Robert M., Former Section Chief, Domestic Terrorism/Counterterrorism Planning Section, Federal Bureau of Investigation. Testimony before the Senate Committee on Environment and Public Works, Subcommittee on Clean Air, Wetlands, Private Property and Nuclear Safety. Mar. 16, 1999.

[70] 65 *Federal Register* 48107-48133.

[71] The number of available reading rooms appears to have varied over time, and their location is not always easy to determine. Several telephone calls were necessary before CRS identified a reading room near Maine.

[72] EPA Fact Sheet. "Chemical Safety Information, Site Security and Fuels Regulatory Relief Act: Public Distribution of Off-Site Consequence Analysis Information." EPA 550-F00-012, Aug. 2000.

The 1999 Act also directed GAO to report to Congress within three years (i.e., before August 2002) on "the adequacy of chemical information required to be submitted to local emergency response personnel to help them respond to chemical incidents, the adequacy of the delivery of that information, and the level of compliance with the requirement to submit the information."[73] That report was released July 31, 2002. GAO concluded that EPA officials believe industries generally are complying with reporting requirements. GAO's conclusions about the adequacy of information and its delivery were tentative and could not be generalized to the universe of LEPCs.

DOJ also was directed to report to Congress within three years on the extent to which RMP regulations led to actions "that are effective in detecting, preventing, and minimizing the consequences of releases of regulated substances that may be caused by criminal activity," the vulnerability of facilities to criminal and terrorist activity, "current industry practices regarding site security," and security of transportation of substances listed under CAA Section 112(r)."[74] The law directed DOJ to consult with state, local and federal agencies, affected industry, and the public in preparing the report, and to submit any recommendations to Congress. An interim report was due within one year of enactment (i.e., by August 2000), and a final report within three years of enactment (i.e., by August 2002). DOJ missed both deadlines. The Natural Resources Defense Council (NRDC) filed a lawsuit against DOJ March 11, 2002, asserting that DOJ unlawfully withheld or unreasonably delayed the report's submission to Congress.[75] The interim report was released to Congress May 30, 2002, but withheld from the public. On June 3, 2002, DOJ filed a motion to dismiss the NRDC lawsuit. The NRDC moved to dismiss its lawsuit on July 1, 2002.

A GAO study released October 10, 2002, concluded that DOJ failed to complete the mandated study, and that the Department had the funds to do so, although it had no specific appropriation. "Generally, when Congress imposes a new requirement on an agency but does not appropriate funds specifically to implement it, the agency must use existing appropriations to fund the requirement."[76]

After September 11, 2001

Administrative Initiatives. The events of September 11, 2001, bolstered the view that access to information about facilities should be restricted if it might make them more vulnerable to terrorist attacks. This led EPA to limit Internet access on its website to "sensitive" data.

---

[73] U.S. GAO. *Chemical Safety: Emergency Response Community Views on the Adequacy of Federally Required Chemical Information*. July 31, 2002. GAO-02-799. Washington, DC: U.S. Govt. Print. Off. 23 pp.

[74] 42 USC 7412(r)(7)(H)(xi).

[75] *Natural Resources Defense Council v. Ashcroft*, D.D.C., No. 02-0449, Mar. 11, 2002.

[76] U.S. GAO. *Homeland Security: Department of Justice's Response to Its Congressional Mandate to Assess and Report on Chemical Industry Vulnerabilities*. Oct. 10, 2002. GAO-03-24R. Washington, DC: U.S. Govt. Print. Off. 11 pp. At [http://www.gao.gov/new.items/d0324r.pdf], visited July 14, 2005.

Early in October 2001, EPA removed from its website facility-specific information of a general nature that had been compiled from the executive summaries of risk management plans — for example, about the physical state and concentrations of chemicals at facilities and the duration of a possible chemical release — which previously had been considered acceptable for Internet posting. That information remained available on the Internet through OMB Watch's Right-to-Know Network (RTK NET),[77] but EPA refused repeated requests (including a formal FOIA request) to provide updated information about facility plans. EPA released that information only after OMB Watch filed a complaint in the U.S. District Court for the District of Columbia. In July 2005, EPA provided the electronic database to OMB Watch, which promptly made it accessible on its website.[78]

In March 2002, EPA restricted access to Envirofacts, a link to several EPA databases that allowed the user to access facility-specific information about chemical releases, compliance with environmental laws, and other issues. The next week, the White House sent a memorandum to all federal agencies, ordering them to further review and protect information that might be used to threaten national security or public safety. On May 6, 2002, President Bush signed an administrative order granting the EPA Administrator the authority to classify as "secret" information that might pose a national security risk.[79]

On the other hand, the attacks of September 11 led to increased communication among government officials at all levels, as well as facility owners and operators. For example, EPA advised pesticide companies and applicators to be especially vigilant about physical security of chemicals and equipment. The Agency issued a "chemical safety alert" tailored to the security needs of the pesticide industry, based on an earlier paper on site security of chemical plants that first was issued in February 2000.[80] In September 2002, EPA also sent about 9,400 drinking water utilities advice about securing facilities from terrorists. (About 2,000 drinking water utilities submit risk management plans that include worst-case scenarios under the CAA Section 112(r).)

In February 2003, the White House released The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. It outlines goals, principles, "a unifying structure," roles and responsibilities, and the major cross-sector and sector-specific initiatives of national efforts to secure infrastructures and "assets vital to our public health and safety, national security, governance, economy,

---

[77] OMB Watch is a nonprofit research and advocacy group dedicated to promoting government accountability and public participation in public policy decisions.

[78] The recently updated executive summaries of risk management plans submitted to EPA may be examined using RTK NET at [http://www.rtknet.org/rmp/wgrmp.php], visited July 15, 2005.

[79] 67 *Federal Register* 31109, May 9, 2002.

[80] The alerts are available through the EPA website at [http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/ap-chsa.htm], visited Jan. 11, 2006.

and public confidence."[81] Chemical facilities are addressed in connection with three critical infrastructure sectors: the chemical industry and hazardous materials, water, and energy. EPA was the designated lead federal agency for the chemical industry and water, while the Department of Energy (DOE) was the designated lead agency for energy.

With respect to the chemical industry and hazardous materials, the Strategy acknowledged both the potential economic consequences of a successful attack on the sector and the potential threat to public health and safety. It aimed to assure supply to downstream users of chemical products, to protect and assure the quality of chemical stockpiles, and to reduce the risk of malicious use of inherently hazardous chemicals. The Strategy noted that "there is currently no clear, unambiguous legal or regulatory authority at the federal level to help ensure comprehensive, uniform security standards for chemical facilities."[82] In particular, the Strategy observed that federal laws might be out-of-date and no longer effective for monitoring and controlling access to dangerous substances. The President proposed that DHS, in concert with EPA, should "work with Congress to enact legislation to require certain 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."[83] The Strategy also proposed that EPA, in concert with DHS, should review current laws and regulations pertaining to "the distribution and sale of highly toxic pesticides and industrial chemicals." Finally, the Strategy suggested that DHS and EPA should encourage participation in the chemical sector's Information Sharing Analysis Center. The fact that security can be expensive also was noted.

The Strategy described the importance of water from a public health and an economic standpoint and noted that security of the water sector against terrorism had been greatly enhanced since September 11, 2001. Challenges facing the water sector, according to the Strategy, included the need to protect against intentional release of toxic chemicals so as to protect the safety of people who reside or work near water facilities. The Strategy proposed that EPA and DHS identify better ways to secure key points of storage and distribution; improve monitoring and analysis, information exchange, and contingency planning; and manage risks due to interdependencies with other critical infrastructures.

The energy sector was divided into two sections: electricity and the oil/natural gas industries. Overall, energy was described as "essential to our economy, national defense, and quality of life."[84] The Strategy proposed that DHS and DOE work with state and local governments and industry to identify "appropriate levels of

---

[81] Bush, George W. Cover letter to *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Feb. 2003. 83 pp. At [http://www.whitehouse.gov/pcipb/physical.html], visited Jan. 11, 2006.

[82] Ibid., p. 65.

[83] Ibid., p. 66.

[84] Ibid., p. 50.

redundancy" and requirements for "designing and enhancing reliability." In addition, DHS and DOE were to work with oil and natural gas industry representatives to "define consistent criteria for criticality, standard approaches for vulnerability and risk assessments," and "physical security training for industry personnel."[85] An advisory task force was to be convened by DHS and DOE to identify appropriate planning requirements and approaches. Finally, the Strategy proposed that DHS and DOE work with industry "to develop regional and national programs for identifying spare parts, requirements, notifying parties of their availability, and distributing them in an emergency." There is no mention in this section of the hazardous chemicals present in some facilities in the energy sector.[86] However, it may be the Administration's intention that certain facilities, such as oil refineries, electric/gas utilities, and bulk storage facilities, would be included in, and targeted by initiatives in, multiple critical infrastructure sectors.

As the war began in Iraq, the President launched Operation Liberty Shield, a surveillance program to provide additional security for potentially threatened facilities in the critical infrastructure. Chemical plants were among the potential focal points of the initiative.

On December 17, 2003, the President issued Homeland Security Presidential Directive (HSPD) 7, transferring to DHS all EPA authority for overseeing the security of chemical facilities, with the single exception of drinking water and water treatment plants. In addition, the directive revised the Administration's strategy for protecting critical infrastructure by designating DHS the lead agency for the chemical sector. The directive requires that DHS "identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction" (HSPD 7, paragraph 12). In addition, DHS must conduct or facilitate vulnerability assessments of the chemical sector and "encourage risk management strategies to protect against and mitigate the effects of attacks." Finally, all departments and agencies are directed "to work with sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism" and to cooperate with the DHS Secretary.

Private Sector Initiatives. Although trade associations for the chemical industries have been engaged in emergency planning for many years, and began developing guidelines for site security at least a year before September 11, 2001, the events of that date infused on-going efforts with commitment and energy that previously were not evident.

The American Chemistry Council (ACC, formerly the Chemical Manufacturers Association), the Chlorine Institute, Inc., and the Synthetic Organic Chemical Manufacturers Association issued *Site Security Guidelines for the U.S. Chemical Industry* on October 23, 2001. The guidelines build on "Management Practice 15:

---

[85] Ibid.

[86] However, the first of the eight guiding principles underpinning the strategy is "assure public safety, public confidence, and services."

Site Security" in the Responsible Care® Employee Health and Safety Code. Responsible Care® is the ACC's response to general public concerns about the manufacture and use of chemicals. Members of the ACC are required to commit to the principles of Responsible Care® and "to support a continuing effort to improve the industry's responsible management of chemicals" by continually improving their health, safety and environmental performance; listening and responding to public concerns; assisting other companies to achieve optimum performance; and reporting their goals and progress to the public."[87] There are today about 130 corporate ACC members operating approximately 2,000 chemical facilities, representing almost 90% of U.S. chemical productive capacity.[88] About half of the ACC facilities are covered by the CAA Section 112(r) requirements for risk management planning.[89] The ACC guidelines for site security are general, and must be adapted by chemical companies to meet site requirements.

During April 2002, ACC circulated a draft of a Security Code of Management Practices —

> ... to help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities, and maintain and improve relationships with key stakeholders.[90]

On June 5, 2002, the ACC Board of Directors approved the code and voted to make it mandatory for ACC members. Under the Security Code, ACC members are required to evaluate site security using vulnerability assessment methodology equivalent to that developed by the Department of Energy's Sandia Laboratories for the Department of Justice[91] or by the Center for Chemical Process Safety (an industry-funded research center). They are then required to implement security enhancements commensurate with the risks identified by the assessments. Other key requirements of the code include

- training and drills for employees, contractors, customers, and suppliers;
- consideration of process changes, material substitutions, and other inherently safer approaches to chemical production;
- evaluation, response, and reporting of security threats; and

---

[87] The principles of Responsible Care® are listed on the ACC website at [http://www.americanchemistry.com/s_acc/sec_statistics.asp?CID=176&DID=304/], visited Jan. 11, 2006.

[88] Durbin, Martin. Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs, July 13, 2005.

[89] Durbin, Martin. Personal communication. Feb. 4, 2005.

[90] ACC. Responsible Care® Security Code of Management Practices Draft Concepts, Apr. 18, 2002.

[91] National Institute of Justice, U.S. Department of Justice. *Chemical Facility Vulnerability Assessment Methodology*, NCJ 195171, July 2, 2002. At [http://www.ojp.usdoj.gov/nij/pubs-sum/195171.htm], visited Jan. 11, 2006.

- internal audits.[92]

ACC members began by assessing security, including computer security, at high-risk facilities, as well as from supplier to manufacturer, to wholesaler, to retailer, and finally to customer. On March 7, 2003, ACC announced that all of its member companies had completed site vulnerability assessments for their 120 highest priority facilities, prior to the end of 2002, a deadline established by the industry's security code.[93] In early 2005, ACC announced that members had completed implementation of security measures at all 2,040 of their facilities. However, the security code does not require specific expenditures for risk reduction; rather, it recommends decisions should be based on an evaluation of risks and costs. According to ACC, facilities have spent more than $2 billion since September 11 to improve security.[94]

In addition to developing guidelines and a management code on site security, ACC and other chemical trade organizations have been communicating extensively with one another and with government officials about how to reduce the risks of chemical terrorism. For example, ACC and the Association of American Railroads formed a task force to develop strategies to ensure the safety of communities near chemical and rail facilities.[95] In addition, as mentioned above, the Center for Chemical Process Safety has developed a risk-based methodology for assessing the vulnerability of chemical facilities to terrorist attacks. The Synthetic Organic Chemical Manufacturers Association (SOCMA) has developed a vulnerability assessment methodology for smaller chemical producers.[96] In addition, SOCMA has adopted the ACC security code as a condition of membership. According to Tom Hall, director of stewardship for CropLife America (a pesticide industry trade association), pesticide and fertilizer distributors represented by CropLife America, the Fertilizer Institute, and the Agricultural Retailers Association formed a working group to tailor a vulnerability assessment methodology for rural facilities, where theft is a greater threat than a direct attack on a facility.[97] A document, *Guidelines to Help Ensure a Secure Agribusiness*, was released October 24, 2002.[98] Finally, the

---

[92] Responsible Care® website. At [http://www.americanchemistry.com/s_acc/sec_article.asp?CID=258&DID=1232], visited Jan. 11, 2006.

[93] ACC. "Chemical Makers Complete Priority Site Vulnerability Assessments, Continue Security Performance Through Responsible Care®." Press release, Mar. 7, 2003. At [http://www.accnewsmedia.com/docs/1100/1090.doc?DocTypeID=4&TrackID=], visited July 9, 2005.

[94] American Chemistry Council. News & Media website. Security. At [http://www.accnewsmedia.com/site/page.asp?TRACKID=&VID=1&CID=361&DID=1313&PSID=ACC], visited July 9, 2005.

[95] "ACC Teams up with Railroad Association to Boost Chemical Security," *Pesticide & Toxic Chemical News Daily*, vol. 4, no. 5, Mar. 28, 2002, p. 2.

[96] DeConti, Angela. Personal communication, July 9, 2002.

[97] Hall, Tom. Personal communication, July 2, 2002.

[98] The Guidelines may be accessed through the Internet at [http://www.aradc.org/secure

(continued...)

American Petroleum Institute has published security guidelines developed in consultation with the Department of Energy.

GAO examined the voluntary initiatives underway in a report released in March 2003, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities but the Extent of Security Preparedness Is Unknown*.[99] GAO concluded that many initiatives are admirable, but "the extent of security preparedness at U.S. chemical facilities is unknown ... [because] no federal requirements are in place to require chemical facilities to assess their vulnerabilities and take steps to reduce them ... [and] no federal oversight or third-party verification ensures that voluntary industry assessments are adequate and that necessary corrective actions are taken."

Congressional Action. The 107th Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188), which requires many community water systems to perform vulnerability assessments and to prepare emergency preparedness and response plans. Some of these facilities handle significant quantities of hazardous chemicals. Funding is authorized to assist communities in complying with the act. It also directs EPA to review methods to prevent, detect, and respond to threats to water safety and infrastructure security. P.L. 107-117 provided EPA with roughly $90 million to enhance the security of drinking water treatment facilities.

The 107th Congress also enacted the Maritime Transportation Security Act (MTSA, P.L. 107-295), which requires the DHS Secretary to identify port facilities "that pose a high risk of being involved in a transportation security incident," and to conduct a vulnerability assessment of such facilities. Facility owners or operators are required to develop and submit to DHS both security plans and incident response plans that deter "to the maximum extent practicable a transportation security incident or a substantial threat of such a security incident"; are consistent with national and area security plans; and conform to requirements specified by the U.S. Coast Guard. DHS must review and approve each plan. The act also authorized a grant program that finances security upgrades. For more information about the MTSA and related issues, see CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*, by John Fritelli.

P.L. 107-296, establishing DHS, does not address chemical plant security directly. However, the law does require DHS to analyze vulnerabilities and recommend methods of enhancing site security at facilities that are part of the "critical infrastructure." As noted above, the Administration has identified chemical facilities as part of the critical infrastructure in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Chemical facilities are included in several sectors: water utilities, the energy sector, and the chemical and hazardous materials sector. The law exempts from public disclosure requirements

---

[98] (...continued)
agribusinessguidelines.pdf], visited Jan. 11, 2006.

[99] U.S. GAO. *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities but the Extent of Security Preparedness is Unknown.* Mar. 2003. GAO-03-439. 41 pp. At [http://www.gao.gov/new.items/d03439.pdf], visited Jan. 11, 2006.

(i.e., FOIA) any information about physical and cyber security if it is submitted voluntarily to DHS by such facilities for use by that agency related to "the security of critical infrastructure and protected systems." Disclosure under the authority of state or local laws also is prohibited. Unauthorized disclosure of "critical infrastructure information" by government employees is punishable by imprisonment, fines, and removal from office.

The 108th Congress amended the MTSA in the Coast Guard and Maritime Transportation Act of 2004, P.L. 108-293, on August 9, 2004. Title VIII of that act requires the DHS to submit a plan for a maritime security grant program, including recommendations on how funds should be allocated.

Policy Options

September 11, 2001 prompted policy makers to reconsider federal policy options regarding potential terrorist threats to chemical facilities. A range of possible strategies is summarized below. Additional information on this topic is provided by CRS Report RL33043, *Legislative Approaches to Chemical Facility Security*, by Dana A. Shea.

Status Quo. Congress might rely on existing mechanisms in the public and private sectors to continuously evaluate and improve site security. Federal statutes already mandate facility assessments of chemical hazards and planning to prevent, mitigate, and respond to accidental releases of hazardous chemicals. And the events of September 11, 2001, undoubtedly have reinvigorated implementation efforts by federal, state, and local government officials, as well as facility operators. Some state and local governments have instituted additional security requirements. For example, Baltimore, Maryland, requires chemical facilities to implement security measures described by police and fire officials. Moreover, trade associations have developed vulnerability assessment methodologies to facilitate planning for diverse types of facilities. The ACC requires that its members assess vulnerability and devise plans to improve security.

The establishment of DHS and Homeland Security Presidential Directive 7 on the protection of critical infrastructure ensure a federal role in chemical facility security planning. The President directed DHS to identify and prioritize facilities needing protection from terrorists, to facilitate vulnerability assessment and security planning, and to coordinate private, local, state, and federal initiatives to improve security. However, many in Congress and President Bush have stated that the federal government might need additional authority to require security measures at chemical facilities, and called for legislation that would provide that authority.[100]

Collect Additional Information. Another option would be to delay addressing chemical facility security until additional information is gathered on which to base proposals. The final DOJ assessment of chemical site security and the impact of the current risk management planning program might provide needed

---

[100] President George W. Bush. Sept. 10, 2003. "President Bush Discusses Homeland Security at the FBI Academy," FBI Academy, Quantico, Virginia.

insights. For a broader view of the issue, including analysis of policy options, Congress might establish a Blue Ribbon Panel or request a study by the National Academy of Sciences. Studies could provide information about the risks of terrorism, the risks of accidents, the views of public interest groups, and the effectiveness of public disclosure to reduce risks. Such information might assist Congress in evaluating alternative approaches to reducing risks. However, the benefits gained from delaying federal decisions pending development of better risk information should be weighed against the possibility that terrorists might strike this kind of facility before Congress acts.

Improve EPA Guidance and Enforcement. Congress also might provide additional resources for, or exercise increased oversight over, implementation of existing statutes. Although neither EPCRA nor the CAA explicitly addresses chemical releases due to criminal or terrorist acts, EPA arguably has sufficient authority under the acts to more strongly encourage facilities to reduce their vulnerability to terrorists. Additional resources could facilitate EPA review of facility risk management plans. Through September 2001, EPA had reviewed only 15% of submitted plans, according to a GAO report.[101]

As previously mentioned, EPA already has provided guidance to facilities on this subject, but many public interest groups would like EPA to go farther in interpreting the risk management planning requirements of the CAA Section 112(r).[102] For example, US PIRG argued in a 1998 report:

> EPA missed opportunities to require companies to identify inherently safer technologies, and ignored comments made by a coalition of environmental and labor organizations calling for a requirement that companies undertake Technology Options analyses to identify inherently safer technologies.[103]

In lieu of regulations, EPA could be urged to provide technical assistance or demonstration programs, or to develop incentives to encourage risk reduction.

EPA has considered revisions to either the risk management planning rule or EPA guidance under the CAA Section 112(r)(7) to require or encourage chemical facility owners to assess their vulnerability to terrorists and correct any significant weaknesses. Some EPA officials expected new principles for risk management planning to address both site and computer security; building access; background checks; inventory controls; storage safety; and other physical security measures, as well as changes that improve "inherent safety."[104]

---

[101] U.S. GAO, p. 4.

[102] Hind, Rick. Legislative Director, Greenpeace Toxics Campaign. Letter to Christine Todd Whitman, EPA Administrator. March 14, 2002.

[103] Laplante, Allison. *Too Close To Home: A Report on Chemical Accident Risks in the United States*, U.S. Public Interest Research Group, Washington, DC. July 22, 1998.

[104] Heilprin, John. "Government to Require 15,000 Chemical, Waste, Water Plants to Assess Terrorism Risks, Make Fixes," *The Associated Press*, via NewsEdge Insight, June 7, 2002.

However, EPA has stated that its authority to regulate chemical site security is unclear, and authority under the Clean Air Act has been questioned by the House Committee on Energy and Commerce.[105] In October 2002, Administrator Whitman announced that EPA would not pursue chemical security regulations under the CAA.[106] President Bush has made it clear that he does not envision a large role for EPA with respect to security from terrorism. Congress might ultimately elect to clarify EPA authority through legislation, expanding or narrowing current interpretations, or examine the adequacy of EPA's implementation of the risk management planning rule in congressional hearings.

A potential disadvantage of relying on existing law is that it may not apply to all facilities of interest. For example, the CAA, Section 112 applies to chemicals that were selected based on severity of potential acute adverse health effects, the likelihood of *accidental* releases, and the potential magnitude of human exposure. It excludes explosives, as well as flammable substances when used as a fuel, or held for sale as a fuel at a retail facility.

Reduce Risk Through Legislation. GAO has recommended that DHS and EPA, in consultation with the Office of Homeland Security, jointly develop a comprehensive national chemical security strategy, which should include a legislative proposal "to require chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action."[107] DHS and EPA agree.[108] *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* asks DHS to work with Congress to enact such legislation.[109]

If Congress decides that legislation is required to reduce the risks of terrorism targeting chemical plants, proposals might focus on preventing terrorism in general or on reducing risks of terrorism specifically targeting chemical plants. A broad focus on reducing terrorism would involve numerous issues that are beyond the scope of this report. Interested readers are referred to CRS Issue Brief IB10119, *Terrorism and National Security: Issues and Trends*, by Raphael Perl.

A narrower focus on chemical plants might provide incentives for voluntary private sector initiatives or new regulatory authorities to reduce risks. Economists Robert Litan and Peter Orszag have suggested that a blended approach involving performance-based regulation and a requirement for insurance coverage against

---

[105] EPA. 2002. *Lessons Learned in the Aftermath of September 11, 2001.* p. ES-10.

[106] Preston, Meredith. "EPA Announces Strategy to Meet Homeland Protection Responsibility," *Daily Environment Report*, Oct. 3, 2002. p. A-1.

[107] GAO. *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*. March 2003. GAO-03-439. Washington, DC: U.S. Govt. Print. Off. p. 31. At [http://www.gao.gov/new.items/d03439.pdf], visited Jan. 11, 2006.

[108] Ibid.

[109] Bush, George W. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003. p. 66.

terrorist acts might be the most cost-effective approach.[110] Stakeholder views regarding the relative merits of voluntary versus mandatory approaches are discussed in the next major section of this report, Policy Issues, in the subsection on Responsibility and Accountability. Bills under current consideration are described in the last major section of this report, Legislation in the 109th Congress.

The remainder of the present discussion analyzes selected strategies and tactics for reducing risks that may be incorporated into legislation.

Physical Security Enhancement. Perhaps the most common approach to improving site security is to "harden" defenses so that sites would be less vulnerable to terrorists.[111] According to the recently released DOJ vulnerability assessment methodology, an effective protection system serves three functions: detection (discovery or sensing of adversary action), delay (impediment to adversary progress), and response by security personnel to ensure that a threat is neutralized.[112] Examples of hardening tactics include increasing security patrols, strengthening fences, installing better locks on doors, relocating sensitive chemical processes within the facility, installing intruder detection systems and alarms, and performing background checks on employees. Congress has adopted such tactics in other contexts. For example, the USA Patriot Act (P.L. 107-56) requires background checks as a condition for obtaining a license to operate a motor vehicle transporting a hazardous material in commerce.

A key advantage of hardening tactics is their variety and adaptability to a range of security needs. Other advantages include the ability to deepen defenses by adding layers of protection and, in many cases, relatively low costs. A potential weakness of this strategy is that even the most effective security measures might be disabled or overwhelmed by a determined, skilled terrorist organization. For example, guards might be bribed or killed, passwords discovered, alarms short-circuited, or computers hacked. The World Trade Center and Pentagon attacks demonstrate the vulnerability of any site to a novel and vigorous attack.

Technology Assessment and Inherently Safer Options. An alternative strategy for reducing risk is advocated by environmental groups. It would reduce the hazardous characteristics of the facility, for example, by reducing production, processing, storage, and use of dangerous chemicals, or changing the characteristics of chemicals to make them less dangerous (e.g., by reducing volatility). Such tactics aim to improve the "inherent safety" of a site, and are preferred by advocates to target-hardening tactics, which they often refer to as "add-on safety systems."[113] According to this view, "'Inherent Safety' activities reduce or eliminate the possibility of an accident occurring through the fundamental redesign of production

---

[110] Litan, Robert, and Peter Orszag. 2002. A complicated intersection: Public action to protect private property. *Brookings Review*, vol. 20, no. 3 (summer). pp. 20-23.

[111] National Institute of Justice, p. 1.

[112] Ibid., pp. 15-16.

[113] Laplante, Allison. *Too Close To Home: A Report on Chemical Accident Risks in the United States*, U.S. Public Interest Research Group, Washington, DC. July 22, 1998.

systems or products, reductions in chemical inventories, or substitution for hazardous chemicals at the facility."[114] Currently, there is no federal U.S. law that explicitly promotes use of inherently safer technologies (IST) by the chemical industry.

Two potential advantages of this approach are that consequences of terrorism may be reduced even if a terrorist succeeds in his mission, and that risks associated with accidental releases of chemicals also are likely to be reduced. In addition, efforts to promote inherent safety of production could fill gaps in current laws, which address risks associated with specified chemicals and industries. According to the U.S. Chemical Safety and Hazard Investigation Board, many reactive chemicals responsible for industrial accidents are not covered by the CAA Section 112.[115]

The chemical industry developed the concept of inherent safety,[116] and the ACC Security Code requires members to "consider" it in choosing security measures. Many facility operators have applied this approach in recent years. For example, a utility in Ohio chose to employ a urea-based pollution control system instead of another system which would have required storage of large quantities of ammonia.[117] Shortly after September 11, the Blue Plains wastewater treatment facility in Washington D.C. stopped using chlorine in favor of the less volatile sodium hypochlorite bleach.[118] Other water and wastewater treatment plants are making similar changes in chemical usage.

The key disadvantages of this "safer" facility strategy are potentially higher production and research and development costs, delays in achieving security while new processes are put into place, and, at least in some cases, lack of feasibility. However, advocates argue that use of safer technologies may reduce production costs by reducing regulatory burdens, insurance premiums, transportation costs, and waste disposal costs. Another potential disadvantage of the strategy is that some "safer" tactics may simply spread a risk around, shift the risk to other locations or populations, or substitute one risk for another. For example, in replacing an acutely toxic chemical (that produces relatively severe health effects after a short exposure) with a less acutely toxic chemical, one might increase chronic risks (due to low-level, long-term exposures) or environmental risks (e.g., due to the chemical's persistence).

Deterrence. A third approach to reducing risks aims to reduce theft, rather than direct attacks, by making dangerous chemicals in use at a facility less attractive to criminals, for example, by introducing a color or other property that facilitates detection and tracking by authorities (so-called "taggants"), or by creating and storing antidotes to toxic effects. A disadvantage of this approach is that taggants act as contaminants, and therefore may impede chemical processes. For this reason,

---

[114] Ibid.

[115] U.S. Chemical Safety and Hazard Investigation Board website, at [http://www.csb.gov/], visited Aug. 7, 2003.

[116] Bollinger, Robert E., et al., 1996. *Inherently Safer Processes: A Life Cycle Approach*. John Wiley & Sons, Inc., Hoboken, New Jersey. 154 pp.

[117] American Electric Power, press release, Dec. 18, 2000.

[118] "Toxic Chemicals' Security Worries Officials," *Washington Post*, Nov. 12, 2001.

taggants typically are useful only in end products, not in intermediate (i.e., process) chemicals. Generally, such deterrents appear to be in the development stage and are not available for immediate application.

Restricted Access to Information. Restricting terrorists' access to information about vulnerability and location of chemical facilities also might reduce the risk of terrorism. This approach was taken by the 106th Congress when it enacted amendments to the CAA Section 112(r) to prevent Internet posting of risk management plans and worst-case scenarios for accidents. Internet access to information is a particular concern, because it permits anonymous inquiries about sensitive U.S. facilities from remote locations. P.L. 107-296, that established DHS, limits access to sensitive information potentially useful to terrorists by exempting information about critical infrastructures submitted voluntarily to DHS from disclosure requirements of the Freedom of Information Act (FOIA).

A key advantage of restricting access to sensitive information is that it is an inexpensive method of reducing risk. However, some argue that information restriction is contrary to American values, reduces public oversight of chemical facilities and consequently facility operators' incentives to reduce risk, and is not likely to prevent determined terrorist groups from obtaining needed information.[119]

The general issue of public access to facility-specific information is discussed under Key Issues, in the section on Public Disclosure.

Key Issues

Policy makers choosing among policy options for reducing terrorist risks associated with chemical plants are faced with at least three fundamentally political issues: the effect of public disclosure; the relative importance of diverse risks (and associated costs and benefits of risk reduction), and who should be responsible (and held accountable) for achieving results.

Public Disclosure. Public disclosure of information about chemical hazards and risk management plans at industrial facilities is controversial.[120] Professional and trade groups representing the chemical industry oppose the release of information regarding the vulnerability of facilities to terrorism and the potential off-site consequences (OCA) to public health and the environment. They argue that terrorists might use the information to target facilities that are most vulnerable or located near large population centers. Congress responded to this view when it enacted amendments to the CAA Section 112(r) in 1999.

Environmental and right-to-know advocates often oppose restrictions on public disclosure. They argue that communities have a right to be informed about hazards to which they might be exposed, and that free access to information is important to

---

[119] Ament, Lucy. "Greenpeace Maps Possible Chemical accidents," *Pesticide & Toxic Chemical News*, July 1, 2002, p. 9-10.

[120] Davis, Ann. "New Alarms Heat up Debate on Publicizing Chemical Risks," *Wall Street Journal*, May 30, 2002, p. A1.

ensure public accountability of facility managers. Opponents of limiting public information also point out that citizens need information to assess facility compliance with laws, and if necessary, to petition the Administration or the courts for enforcement.[121] Unsafe practices and inadequate risk management plans, in particular, should be publicized, they contend, so that communities may exert political or social pressure on plant managers to improve the inherent safety of their facilities. Moreover, these groups want access to information about similar facilities handling comparable chemicals across the United States, so that plans and accident rates can be compared and analyzed to determine the effectiveness of various safety measures. Informed citizens can work with local plant managers to reduce the risk of accidents, they argue. This view was adopted by Congress in the 1990 amendments to the CAA Section 112(r).[122]

Another argument in favor of public disclosure has been advanced by investment groups, who argue, "Investors need to know about potential liabilities of companies in which they invest."[123] Although some have argued that environmental information is inadequately disclosed, due in part to vague disclosure requirements established by the Securities and Exchange Commission (SEC), the GAO reported in 2004 that the situation is not clear.[124] GAO found: (1) "Key stakeholders disagree" about how well SEC has defined the environmental disclosure requirements; (2) "Little is known about the extent to which companies are disclosing" such information in their filings with SEC; and (3) SEC enforcement of environmental disclosure requirements may or may not be adequate.

With respect to the possibility that information may be used by terrorists, right-to-know advocates claim that public disclosure of chemical hazards motivates facility operators to reduce chemical hazards, thereby reducing the likelihood and severity of harm from terrorist attacks, as well as the risk of chemical accidents.

The net effect on risk to public health and the environment of public disclosure, therefore, appears to depend on the relative risks of releases due to accidents, versus those due to terrorism, and on the extent to which those risks are reduced or enhanced by publication of risk management plans and similar information. However, data are not available to calculate risks, relative risks, or risk reduction/enhancement potential.

---

[121] American Association of Law Libraries, American Library Association, et al. Letter to U.S. Senators, July 12, 2002.

[122] "Coalition says response to terrorism should not limit access to information," *Chemical Regulation Reporter*, vol. 25, no. 45, Nov. 12, 2001. p. 1654.

[123] Frieder, Julie (Calvert), Adam Kanzer (Domini Social Investments), Kathy Leonard (Center for Responsible Investing), Sam Pierce (Ideals Work, Inc.), Steven J. Schueth (First Affirmative Financial Network), Kenneth Scott (Walden Asset Management), Conrad MacKerron (As You Sow Foundation), and Alison L.F. Wise (Progressive Asset Management). Letter to U.S. Senators, July 11, 2002.

[124] U.S. GAO. *SEC Should Explore Ways to Improve Tracking and Transparency of Information*. July 14, 2004. GAO-04-808. Washington, DC: Govt. Print. Off. 80 pp.

A related issue is the extent to which federal laws regarding public disclosure should preempt state and local disclosure laws. P.L. 107-296, establishing DHS, prohibits release under the authority of state and local disclosure laws of "information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems." For more on issues related to information disclosure, see CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security*, by John D. Moteff and Gina Marie Stevens.

Relative Risks. Another important issue involves the diverse and sometimes conflicting goals implicit in discussions of chemical site security enhancement; there is general agreement that risks should be reduced and that "the greatest risks" should be addressed first, but little discussion of which risks are "greatest" and should be targeted and at what cost. For example, should we focus on lowering death rates or rates of sickness and disability? Should we focus on preventive measures or emergency response and recovery services? Should we allocate resources to prevent worst-case scenarios, or everyday risks that add up over time? Are risks due to chemical terrorism worse than risks of equal or greater magnitude due to explosions or firearms? Should we emphasize measures to reduce terrorist risks that also may improve federal efforts to prepare for and respond to other disasters, as the President's National Strategy suggests?[125] To what extent are we willing to sacrifice access to information about facilities in our neighborhoods, privacy, or government accountability for the sake of risk reduction? Are we willing to shift federal resources to DHS and away from other programs? The answers to such questions depend on value judgments and are likely to lead to diverse policy approaches and decisions about particular federal initiatives to reduce the threat of terrorism.

For example, on the one hand, it often is argued that federal expenditures are most efficient when they are allocated with respect to relative risks and risk reduction opportunities. According to this view, relatively more federal funding should be provided to programs targeting risks that are greater and more clearly documented (e.g., to prevent smoking or motor vehicle accidents), than for programs targeting small, hypothetical risks (e.g., from exposure to pesticide residues on food). Based on this reasoning, the risks of chemical terrorism in the United States would deserve relatively few resources, because they are hypothetical and very small. This is especially true for individual chemical facilities. Such reasoning might leave some chemical facilities vulnerable to attack. As explained by the President of the Louisiana Chemical Association, "Worst-case scenarios are just that Virtually every safety system in every process would have to fail for a worst-case scenario to actually happen."[126] Will the federal government or some plant operators find such a scenario incredible, and thus, not worth additional security investments? What cost is justified for risk reduction at individual chemical facilities?

---

[125] Office of Homeland Security. *National Strategy for Homeland Security*, July 2002. p. 3.

[126] Johnson, Jeff. Chemical accident debate rolls on. *Chemical and Engineering News*, Apr. 9, 2001. p. 22. At [http://pubs.acs.org/cen], visited Aug. 6, 2003.

On the other hand, some have argued that the distribution of risk is more important than the absolute or relative magnitude of risk. Scholars at the Brookings Institution, for example, argue that federal resources to combat terrorism should be devoted primarily to avoiding or mitigating potentially catastrophic terrorist acts.[127] Catastrophic events, in which many people are killed or injured at once often strain local social, political, and economic systems, as well as emergency response resources, as was well illustrated by the attack on the World Trade Center and again during the hurricane season of 2005. Thus, the Brookings report focuses on protecting against nuclear, chemical, or biological terrorism and large-scale attacks at airports, seaports, nuclear and chemical facilities, stadiums, big commercial buildings, monuments, and American icons, as opposed to preventing numerous smaller attacks that might produce an equal number of casualties over a longer period of time.

President Bush has directed the DHS Secretary to set priorities for critical infrastructure protection "with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction," but with consideration of numerous other potential effects of terrorist acts. As a result, DHS has been developing a vulnerability-assessment tool, working its way through, "in priority order, first with the nuclear energy sector, and with the chemical sector, and shortly to follow many others across the top tier of consequences, vulnerabilities and threats."[128]

Still others object to reliance on any form of cost-benefit accounting with respect to public health and environmental risk management, because quantitative, analytic tools often do not consider risk factors and management options that they consider important.[129] For example, one cannot produce a reliable estimate of benefits that might accrue from basing decisions on the so-called "precautionary principle" or most other preventive management tools, because specific kinds of damages and clean-up costs may never occur, and thus cannot be validated or corrected. Moreover, it can be argued that quantitative analysis is biased against preventive measures, because the hypothetical benefits, as well as the hypothetical risks, accrue (or not) in the future and generally are discounted (reduced in value). Many observers feel this kind of process inevitably estimates that preventive options will have relatively high short-term costs and relatively low and uncertain long-term benefits.

---

[127] O'Hanlon, Michael E., Peter R. Orszag, Ivo H. Daalder, et al. 2002. *Protecting the American Homeland: A Preliminary Analysis*, Brookings Institution Press, Washington, DC. 177 p.

[128] Stephan, Robert. Testimony before the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Homeland Security Committee, June 15, 2005.

[129] For more on policy issues related to risk analysis and cost-benefit analysis, see CRS Report 98-618, *Environmental Risk Analysis: A Review of Public Policy Issues*, by Linda-Jo Shierow.

Responsibility and Accountability. Deciding who should be responsible for achieving results (or who should be held accountable) requires consideration of many factors, including statutory authority, resource availability, technical competence, political feasibility, and moral or ethical constraints. Responsibility is multifaceted, involving financial, operational, and managerial duties, and may be layered hierarchically. In addition, responsibility may be shared or distributed among several private and public entities. For example, in the case of chemical plant safety, responsibility probably will be divided in some manner to include owners/operators of facilities, insurers, and some unit of government. It is up to policy makers to decide upon the appropriate distribution of each component.

Generally, people agree that the federal government is responsible for protecting citizens and the homeland, and that business owners are responsible for not causing hazards for their employees, neighbors, and assets. However, people have different views about who should be held accountable for the consequences of an act of terrorism, what level of protection from risk is acceptable, whether the private sector is likely to achieve that level of protection without public assistance or oversight, and who should bear the costs of achieving greater safety. These different views largely reflect general political philosophies (e.g., regarding the appropriate role of government and the value of public involvement in risk management decisions), but they also are influenced by specific knowledge of, and attitudes toward, the chemical industry, EPA, and other governmental and non-governmental entities.

Some argue that the risks of terrorism for individual chemical facilities are so small that many facility managers are unlikely to invest sufficient resources to adequately ensure site security. Based on this view, some argue that sufficient reductions in terrorist risks for the nation as a whole can be assured only if chemical facilities are required to comply with federal standards for risk management — that is, if they are held accountable by government. Federally mandated standards are likely to ensure a greater level of safety, according to this view, because administrative rule-making procedures provide for public comments, including comments by people potentially at risk if a terrorist attacks, but who do not directly profit from neighboring facilities. Voluntary chemical site security measures advocated by trade associations do not suffice, it is argued, because they do not cover all potentially dangerous facilities and have no standards, no timelines, no hazard reduction policies, no measurable hazard reduction goals, no accountability, and are not enforceable.[130] However, at least some trade associations require independent audits of risk management plans, as discussed below.

Recent testimony by Robert Stephan, Assistant Secretary of Infrastructure Protection, indicates that approximately 20% of chemical facilities that are relatively hazardous are not voluntarily signed up to an industry security code and are not

---

[130] Orum, Paul. Additional testimony in response to questions from Senator Jon Corzine concerning the Chemical Security act, S. 1602, Jan. 15, 2002, at [http://crtk.org/detail.cfm?docID=243&cat=spills%20and%20emergencies], visited Jan. 11, 2006.

covered by MTSA.[131] As a result, DHS does not know whether they are acting to secure themselves from terrorist acts.

If Congress decides that the private sector must be held accountable, legislation could be enacted authorizing EPA or DHS to conduct or oversee facility vulnerability studies or to set standards for facility risk management. The American Chemistry Council supports enactment of legislation authorizing oversight by DHS. In the 109th Congress, H.R. 1562 and S. 2145 would require submission of vulnerability assessments and security plans to DHS, while H.R. 2237 would require submission to EPA.

Others contend that chemical facility operators are willing and prepared to reduce significant risks, for personal, professional, and business reasons.[132] They argue that well-managed businesses routinely assess, prioritize, and manage risks of all kinds, including risks of potential exposure to hazardous chemicals due to criminal or terrorist acts. Business incentives to good chemical risk management include reduced legal liability, reduced insurance costs, enhanced reputation, improved employee relations, and reduced costs for remediation and victim compensation. In the United States, environmental and occupational health and safety laws provide additional incentives to many facility operators to responsibly manage hazardous chemicals.

Some are opposed to new legislation, because it might disrupt and delay installation of security enhancements by individual companies. On the other hand, if such legislation were enacted, it could benefit businesses by shifting liability to the government and discouraging states from adopting diverse regulatory strategies.

Some industry representatives, while acknowledging that some guidance, training, and financial assistance for threat assessment and risk management are needed, especially for addressing risks to small businesses, point out that trade associations and industrial research centers have been working for several years to fill such needs. Such groups advocate a flexible, risk-based approach to securing facilities, arguing that "most plants are not likely terrorist targets."[133] Some business groups argue that most regulations inappropriately force diverse enterprises to adopt a "one-size-fits-all" strategy. To satisfy any public demand for assurance that risk reduction is occurring, some industry representatives have recommended a safety certification process and are willing to submit their facilities to independent audits.

In the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released in February 2003, the Bush Administration recommended

---

[131] Stephan, Robert. Testimony before the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Homeland Security Committee, June 15, 2005.

[132] Zahodiakin, Phil. 2002. "Industry sees few unturned stones in anti-terror effort," *Pesticide & Toxic Chemical News*, Mar. 18, 2002, p. 10.

[133] Ibid.

legislation to enhance security measures at chemical facilities,[134] although it had hoped to avoid that approach, according to the Secretary of the Department of Homeland Security, Tom Ridge.[135] He acknowledged that the Administration (as of mid-July 2002) had been leaning toward a voluntary approach.[136] The Administration would assign financial responsibility to chemical facility owners. According to Ridge, "[T]his is a cost [chemical companies] have to absorb." For their part, some pesticide trade groups would welcome increased government assistance in the form of funding for education.[137]

Administrative support for legislation again was expressed at a Senate hearing June 15, 2005. Although this was interpreted by many news reports as a change in Administration policy,[138] Robert B. Stephan, Acting Undersecretary of DHS for Information Analysis and Infrastructure Protection, testified that there has been no change in the Administration's position: It has always been willing to work with Congress to produce new regulatory authority to enhance the security of chemical facilities. However, the Undersecretary emphasized that the Administration will only support risk-based regulation of chemical security. Mr. Stephan stated that DHS was not quite ready to propose or approve of any particular legislative provisions, but would be in a position to do so soon.[139]

Legislation in the 109th Congress

Background: 108th Congress Activity. S. 994 was introduced by Senator Inhofe, the Chairman of the Senate Committee on Environment and Public Works, which reported the bill as amended. The bill saw no further action and has not been introduced into the 109th Congress. However, it is the only chemical facility security bill that has been reported to date, and Members continue to refer to it in discussions about current proposals.

In accord with the views of the Bush Administration, S. 994 would have authorized DHS to oversee vulnerability assessments and security and emergency response plans for facilities designated by the DHS Secretary. S. 994, as reported, would have required the Secretary to promulgate regulations directing owners and operators of listed facilities to conduct vulnerability assessments, identify hazards, prepare security plans to reduce vulnerability to a terrorist release and to respond in

---

[134] Bush, George W. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003, p. 66.

[135] Preston, Meredith. "Administration Wants to Avoid Legislation Requiring Safety Measures at Chemical Sites," *Daily Environment Report*, July 11, 2002, p. A-6.

[136] Ibid.

[137] Ibid.

[138] Hall, Mimi. Chemical Plants Need More Protection, Official Says. *USA Today*, June 15, 2005, p. A8

[139] Stephan, Robert. Statement before the U.S. Senate Committee on Homeland Security and Governmental Affairs. June 15, 2005. At [http://hsgac.senate.gov/_files/TestimonyStephan.pdf], visited July 9, 2005.

the event of a release, and update assessments and plans periodically. Written certification of compliance would have been required by DHS from each owner or operator, on a schedule to be determined by the Secretary. As reported, S. 994 would have required owners and operators to submit copies of vulnerability assessments and plans to DHS.

S. 994 would have directed DHS to conduct, or required the conduct of, vulnerability assessments and to evaluate and ensure compliance with promulgated regulations. Vulnerability assessments and plans would have been protected from public disclosure under FOIA and state and local disclosure laws. Criminal penalties were provided for unauthorized, knowing disclosure by federal officials. Although S. 994, as reported, would not have required DHS to review and approve assessments and plans, DHS would have been authorized to disapprove any assessment or plan, and to order revision if it did not comply with regulations, or if the plan or implementation were insufficient to address the results of a vulnerability assessment or a threat of a terrorist release. The Secretary would have been required to provide notice of disapproval explaining deficiencies, and to identify appropriate steps to achieve compliance. S. 994 would have required the Secretary to issue a compliance order if a plan were disapproved and compliance had not been achieved by a date determined by the Secretary to be appropriate. Such orders would have been protected from public disclosure. Civil, but not criminal, penalties would have been available if facility owners or operators failed to comply with an administrative order. The bill also would have authorized the Secretary to provide training relevant to the legislation to state and local officials and facility owners or operators.

109th Congress Activity. The shape of legislation and its fate in the 109th Congress may be affected by a shift in committee structure in both the House and the Senate. The recently renamed Senate Committee on Homeland Security and Governmental Affairs has taken the lead in holding hearings and developing legislation in the Senate. In the House, it is not clear whether jurisdiction over chemical facility security continues to rest with the Committee on Energy and Commerce, which held hearings during the 108th Congress, or whether it has been transferred in whole or in part to the newly permanent Committee on Homeland Security.

H.R. 2237. In the House, two chemical facility security bills have been introduced; both are similar to proposals in the 108th Congress. H.R. 2237 (introduced by Representative Pallone and similar to S. 157/H.R. 1861 in the 108th Congress) would build on existing EPA authority to oversee chemical facilities but would require consultation with DHS. It would require EPA to designate "certain combinations of chemical sources and substances of concern" as high priority categories based on the severity of the threat posed by an unauthorized release, proximity to population centers, and other criteria. Owners and operators of facilities within high priority categories would be required to conduct vulnerability assessments, identify hazards, and prepare prevention, preparedness, and response plans to eliminate or significantly lessen the potential consequences of an unauthorized release. Plans would be required to incorporate inherently safer technology, if practicable. Copies of vulnerability assessments and plans would be submitted to EPA and updated periodically.

H.R. 2237 would protect vulnerability assessments and plans from public disclosure under FOIA, but the nondisclosure provisions differ considerably from those in P.L. 107-296, establishing DHS. Generally, compared to that law's exemption from FOIA for voluntarily submitted "critical infrastructure information," H.R. 2237 appears to exempt a narrower range of information from disclosure under FOIA, equivalent to exemptions allowed by FOIA itself. In addition, H.R. 2237 would allow disclosure of information under state or local laws, if the state or local government received the information independently of DHS. Also, H.R. 2237 would provide no civil liability immunity for those who submit information nor criminal penalties for unauthorized disclosure.

H.R. 2237 would direct EPA to review each assessment and plan, determine compliance, and certify that determination. EPA would be authorized to issue compliance orders 30 days after notifying a chemical source that its assessment or plan was inadequate and offering compliance assistance, if the plan was not revised to comply with EPA requirements. If DHS notified a chemical source that its plan or implementation was insufficient to address a threat of terrorist attack, and the chemical source took inadequate action in response to that notice, DHS would be authorized to secure necessary relief to abate the threat from a district court in the district where the threat existed.

H.R. 1562. The other House bill, H.R. 1562, was introduced by Representative Fossella. It offers an approach more similar to that of S. 994, as reported in the 108th Congress. H.R. 1562 would make DHS the lead agency overseeing chemical facility security, but it would require consultation between DHS and EPA. The bill would give the DHS Secretary discretionary authority to select facilities that should conduct vulnerability assessments and security planning, but it would require designation of high-priority facilities. H.R. 1562 would exempt from its requirements drinking water treatment facilities required to conduct vulnerability assessment under the Safe Drinking Water Act and facilities subject to the MTSA, unless the owner or operator of such a facility petitioned the Secretary to be subject to the requirements of this act in lieu of the former act. Vulnerability assessments and plans would be focused in H.R. 1562 on security (i.e., hardening) and emergency measures, in order to prevent and respond to releases caused by terrorism, rather than on inherent safety measures that might reduce the consequences of an unauthorized release, regardless of cause.

H.R. 1562 also would protect from public disclosure under FOIA and state and local disclosure laws the certification documents submitted by facility managers indicating that they have complied with assessment, planning, and implementation requirements. (This is in addition to a provision that protects from public disclosure information related to vulnerability assessments and security plans.) H.R. 1562 also would withhold such information from civil judicial or administrative proceedings (except with respect to compliance with the chemical facility security legislation), thus shielding facility owners from lawsuits based on those documents. Criminal penalties are provided for unauthorized knowing disclosure of protected information by government officials.

H.R. 1562 would authorize DHS to disapprove any assessment or plan, and to order revision if it did not comply with regulations, or if the plan or implementation were insufficient to address the results of a vulnerability assessment or a threat of a

terrorist release. Civil, but not criminal, penalties would have been available if facility owners or operators failed to comply with an administrative order.

S. 2145. Senators Collins and Lieberman, Chair and Ranking Member of the Committee on Homeland Security and Governmental Affairs (HSGAC), introduced S. 2145 in late December. S. 2145 would direct the Secretary of DHS to promulgate rules for identifying chemical sources for regulation, assigning sources to various risk-based tiers, and establishing performance-based security standards for each tier. Facilities would be considered for listing if they produced, used, or stored a substance of concern in a quantity equal to or greater than a threshold quantity. Substances of concern would be those that trigger risk management planning under the Clean Air Act, Section 112(r), ammonium nitrate, and any other substance designated by the Secretary based on the potential extent of death, injury, or serious adverse effects to human health and safety or the environment or the potential impact on national or economic security or critical infrastructure caused by a terrorist incident. Designated facilities would be required to certify completion of and submit to DHS vulnerability assessments, security plans, and emergency response plans for terrorist incidents. DHS would be required to review these submissions.

For facilities in the higher risk tiers, S. 2145 would require a DHS decision to approve, disapprove, or modify facility assessments and plans within two years of the date of enactment (within one year of the date when DHS issues regulations concerning assessments and plans). The bill would establish a duty to report for facilities handling more than a threshold quantity of a designated substance of concern, and it would require plans to specify "steps taken by the chemical source to coordinate security measures and plans for response to a terrorist incident with Federal, State, and local government officials, including law enforcement and first responders." Plans would have to be "sufficient to deter, to the maximum extent practicable, a terrorist incident or a substantial threat of such an incident," and "include security measures to mitigate the consequences of a terrorist incident."

S. 2145 would provide administrative, civil, and criminal penalties for facility owners or operators who fail to submit assessment or plans or to implement plans adequately. Persistent noncompliance with the requirements established under S. 2145 would be sufficient cause for DHS to issue an order for the chemical source to cease operation.

The bill would mandate coordination with existing security and emergency response planning, including planning under MTSA. To that end, S. 2145 establishes regional security offices and area security committees and plans. State and local laws would not be preempted unless they were inconsistent with federal law.

DHS and other federal, state, and local agencies would not be required to release to the public vulnerability assessments, site security plans, security addenda to emergency response plans, area security plans, or materials developed or produced exclusively in preparation for assessments or plans. However, the bill would require public disclosure of written certifications of compliance by facility owners/operators, DHS certificates of compliance issued for individual sources, DHS orders issued for noncompliance, and lists of facilities for which DHS has issued an approval or disapproval, unless the Secretary determines that release of a particular record would

increase security risk. Other provisions would require reports by DHS and GAO, establish a process by which any person may submit a report to DHS regarding vulnerabilities of a chemical source, and protect whistle-blowers from retaliation.

Other Legislation. In addition to these comprehensive proposals to enhance the security of chemical facilities, bills have been introduced that address specific categories of chemical facilities. For example, S. 2052/H.R. 713 would provide a tax credit to agricultural businesses for security enhancements, and S. 1995 addresses the security of wastewater treatment facilities.

On July 14, 2005, the Senate unanimously agreed to an amendment to H.R. 2360, the Department of Homeland Security Appropriations Act for 2006, expressing the "Sense of the Senate that Congress should pass legislation establishing enforceable federal standards to protect against a terrorist attack on chemical facilities within the United States." The conference report on H.R. 2360, which became P.L. 109-90 on October 18, 2005, included the same provision and added a requirement for DHS to submit a report to the Appropriations Committees by February 10, 2006, "on the resources needed to implement mandatory security requirements ... and to create a system for auditing and ensuring compliance with the security standards." The conferees also directed the Secretary to complete vulnerability assessments of the highest risk chemical facilities by December 2006 and to complete a national security strategy for the chemical sector by February 10, 2006.

Conclusions

The threat of terrorism in the United States challenges the existing balance maintained in federal laws between the public's right to know about chemical hazards and the chemical industry's right to protect confidential business information. At issue are risks to public health and safety, environmental protection, civil rights and duties, national security, and privacy. Some are advocating a strategy of relative risk analysis and analysis of risk management options to reveal the best course of action. However, information appears to be inadequate for quantitative evaluation of the risks of chemical releases, whether deliberate or accidental, and the nature of terrorism makes prediction difficult. Moreover, there is no universally accepted level of tolerable risk, no obvious basis for a comparison of relative risks and benefits, and no established federal mechanism for ensuring responsible management of the risks of chemical terrorism.

A variety of federal policy options are available for enhancing chemical security. In choosing among options, policy makers face three key issues: how to evaluate the risks versus the benefits of public disclosure; how to determine and prioritize the relative importance of diverse risks; and who to hold responsible for achieving results. Legislative proposals introduced to date in the 109th Congress would require vulnerability assessments for covered chemicals and facilities and implementation of security plans and emergency response plans to address hazards revealed in such assessments, but the proposals differ in other respects. It remains to be seen which proposal, if any, might be enacted.

Additional Reading

CRS Report RL31547. *Critical Infrastructure Information Disclosure and Homeland Security*, by John D. Moteff and Gina Marie Stevens.

CRS Report RL31861. *High-Threat Chemical Agents: Characteristics, Effects, and Policy Implications*, by Dana A. Shea.

CRS Report RL31542. *Homeland Security — Reducing the Vulnerability of Public and Private Information Infrastructures to Terrorism: An Overview*, by Jeffrey W. Seifert.

CRS Report RL33043. *Legislative Approaches to Chemical Facility Security*, by Dana A. Shea.

CRS Report RL31294. *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, by Mary Tiemann.

CRS Report RL32189. *Terrorism and Security Issues Facing the Water Infrastructure Sector*, by Claudia Copeland and Betsy Cody.