United States General Accounting Office

GAO

Report to Congressional Requesters

March 2003

HOMELAND SECURITY

Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown

GAO

Accountability * Integrity * Reliability

GAO-03-439

March 2003

GAO
Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-439, a report to Congressional Requesters

HOMELAND SECURITY

Voluntary Initiatives Are Under Way at Chemical Facilities but the Extent of Security Preparedness Is Unknown

Why GAO Did This Study

The events of September 11, 2001, triggered a national re-examination of the security of thousands of industrial facilities that use or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk of serious injury or death in the event of a terrorist-caused chemical release. GAO was asked to examine (1) available information on the threats and risks from terrorism faced by U.S. chemical facilities; (2) federal requirements for security preparedness and safety at facilities; (3) actions taken by federal agencies to assess the vulnerability of the industry; and (4) voluntary actions the chemical industry has taken to address security preparedness, and the challenges it faces in protecting its assets and operations.

What GAO Recommends

This report recommends that the Secretary of Homeland Security and the Administrator of the Environmental Protection Agency (EPA) jointly develop a comprehensive national chemical security strategy that is both practical and cost effective, which includes assessing vulnerabilities and enhancing security preparedness.

The Departments of Homeland Security and Justice and EPA generally agreed with the report's findings and conclusions and were supportive of efforts to pursue chemical security legislation.

www.gao.gov/cgi-bin/getrpt?GAO-03-439.

To view the full report, including the scope and methodology, click on the link above. For more information, contact John B. Stephenson at (202) 512-3841 or stephensonj@gao.gov.

What GAO Found

Chemical facilities may be attractive targets for terrorists intent on causing economic harm and loss of life. Many facilities exist in populated areas where a chemical release could threaten thousands. EPA reports that 123 chemical facilities located throughout the nation have toxic "worst-case" scenarios where more than a million people in the surrounding area could be at risk of exposure to a cloud of toxic gas if a release occurred. To date, no one has comprehensively assessed the security of chemical facilities.

No federal laws explicitly require that chemical facilities assess vulnerabilities or take security actions to safeguard their facilities from attack. However, a number of federal laws impose safety requirements on facilities that may help mitigate the effects of a terrorist-caused chemical release. EPA believes that the Clean Air Act could be interpreted to provide authority to require chemical facilities to assess their vulnerabilities and to make security enhancements that protect against attacks. However, EPA has not attempted to use these Clean Air Act provisions because of concerns that this interpretation would pose significant litigation risk and has concluded that chemical facility security would be more effectively addressed by passage of specific legislation.

The federal government has not comprehensively assessed the chemical industry's vulnerabilities to terrorist attacks. EPA, the Department of Homeland Security, and the Department of Justice have taken preliminary steps to assist the industry in its preparedness efforts, but no agency monitors or documents the extent to which chemical facilities have implemented security measures. Consequently, federal, state, and local entities lack comprehensive information on the vulnerabilities facing the industry.

To its credit, the chemical industry, led by its industry associations, has undertaken a number of voluntary initiatives to address security at facilities. For example, the American Chemistry Council, whose members own or operate 1,000, or about 7 percent, of the facilities subject to Clean Air Act risk management plan provisions, requires its members to conduct vulnerability assessments and implement security improvements. The industry faces a number of challenges in preparing facilities against attacks, including ensuring that all chemical facilities address security concerns. Despite the industry's voluntary efforts, the extent of security preparedness at U.S. chemical facilities is unknown. Finally, both the Secretary of Homeland Security and the Administrator of EPA have stated that voluntary efforts alone are not sufficient to assure the public of industry's preparedness.

Contents

Letter 1

Results in Brief 3
Background 6
An Attack Against Chemical Facilities Could Cause Economic Harm and Loss of Life 9
No Federal Requirements Specifically Require Chemical Facilities to Address the Threat of Terrorism 12
Federal Agencies Have Not Comprehensively Assessed the Vulnerability of the Chemical Industry to Terrorism, but Have Taken Some Preliminary Steps 18
Chemical Industry Has Taken Actions to Address Security Concerns, but Faces Significant Challenges in Preparing Against Terrorist Attacks 23
Conclusions 30
Recommendations for Executive Action 31
Agency Comments 31

Appendix I **Comments from the Department of Homeland Security** 34

Appendix II **Comments from the Department of Justice** 36

Appendix III **GAO Contacts and Staff Acknowledgments** 41

Table

Table 1: Number and Percent of RMP-Covered Processes by Industry Sector 7

Figure

Figure 1: Number of Facilities with Worst-Case Accidental Release Scenarios by Residential Population Potentially Threatened 10

Abbreviations

ACC	American Chemistry Council
ATSDR	Agency for Toxic Substances and Disease Registry
CCPS	Center for Chemical Process Safety
DEA	Drug Enforcement Agency
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
Justice	Department of Justice
OHS	Office of Homeland Security
OSHA	Occupational Safety and Health Administration
RMP	Risk Management Plan
SOCMA	Synthetic Organic Chemical Manufacturers Association

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

March 14, 2003

Congressional Requesters

As the events of September 11, 2001, showed, terrorists can cause enormous damage to our country by attacking infrastructure essential to our economy and jeopardizing public health and safety. Following these events, the President, in the National Strategy for Homeland Security, identified 13 sectors as critical to the nation's infrastructure.[1] One of the sectors identified—the nation's $450 billion chemical industry—produces the chemicals needed to manufacture thousands of products, such as those used in agriculture, pharmaceuticals, and automobiles. Furthermore, the federal government has identified 140 toxic and flammable chemicals that, in certain amounts, would pose the greatest risk to human health and the environment if they were accidentally released into the air. The chemical industry is not the only U.S. industry that houses these hazardous chemicals. Other industries, such as agricultural retailers, drinking water and wastewater treatment systems, food processors and distributors who have ammonia refrigeration systems, and petroleum refineries, also house these chemicals. In all, the federal government estimates that a total of 15,000 facilities in the United States produce, use, or store more than threshold amounts of these 140 hazardous chemicals.

Even before September 11, 2001, protecting chemical facilities was the shared responsibility of federal, state, and local governments in partnership with the private sector. However, attention was focused largely on the risks of accidental, rather than intentional, chemical releases. The Environmental Protection Agency (EPA), under the Clean Air Act, requires that about 15,000 facilities with more than threshold amounts of chemicals posing the greatest risk to human health and the environment take a number of steps to prevent and prepare for an accidental chemical release. These facilities must develop a risk management program, which includes an assessment of the off-site consequences of an accidental chemical release and an accident prevention program, and an emergency response plan. The events of September 11, 2001, brought heightened attention to chemical facility

[1]The 13 critical infrastructures include agriculture, energy, water, banking and finance, and public health.

security and the possibility of an intentional terrorist-caused chemical release.

The federal government's role in protecting facilities from terrorist attack has been much debated since September 11, 2001. Debate has focused on whether the federal government should impose security requirements on chemical facilities or whether voluntary industry actions are sufficient. Congress is currently considering several legislative proposals that address the protection of critical infrastructure, including mandating security measures at chemical facilities.

As agreed with your offices, we examined a number of issues surrounding the security of the chemical industry. In this report, we (1) summarize available information on the threats and risks from terrorism that U.S. chemical facilities face; (2) describe federal requirements for security preparedness and the safe management of chemicals at these facilities; (3) describe actions federal agencies have taken to assess the vulnerability of the chemical industry or to address security preparedness; and (4) describe the voluntary actions the chemical industry has taken to address security preparedness, and the challenges it faces in protecting its assets and operations. To determine the threats and risks from terrorism faced by U.S. chemical facilities, we interviewed officials at the Department of Defense's Army Office of the Surgeon General and the Defense Threat Reduction Agency. We also interviewed officials in the Department of Justice's (Justice) National Institute of Justice and several units of the Federal Bureau of Investigation (FBI) including the Hazardous Materials Response Unit, the National Infrastructure Protection Center, and the Weapons of Mass Destruction Unit. We interviewed officials at EPA headquarters, including those from the Chemical Emergency Preparedness and Prevention Office, and we reviewed risk management plan (RMP) data. We also collected and reviewed available reports.

To determine the federal requirements for security preparedness and the safe management of chemicals at these facilities, we interviewed officials from the Department of Labor's Occupational Safety and Health Administration (OSHA) and EPA on safety standards and legal authority. We reviewed statutes and regulations to determine the relevant statutory framework. To determine the actions taken by federal agencies to assess the vulnerability of the chemical industry or to address security preparedness, we reviewed the National Strategy for Homeland Security and several Justice reports. We interviewed officials at the Departments of Energy and Justice, at EPA, and at OSHA. We also attended EPA-sponsored training classes on vulnerability assessments taught by officials

from the Department of Energy's Sandia National Laboratories. We also discussed the voluntary actions the chemical industry has taken to address security preparedness and the challenges it faces in protecting its assets and operations with these agencies. In addition, we interviewed the U.S. Chemical Safety and Hazards Investigation Board, the Center for Chemical Process Safety, and numerous industry associations including the American Chemistry Council (ACC), the American Petroleum Institute, the Chlorine Institute, Inc., the Fertilizer Institute, the Gas Processors Association, the International Institute of Ammonia Refrigeration, the National Petroleum and Refiners Association, and the Synthetic Organic Chemical Manufacturers Association. We attended security conferences held by the ACC and the American Petroleum Institute.

We also interviewed industry officials at a number of facility locations. To select the facilities for our visits, we used EPA's RMP database to select facilities in the highest-risk tier in states with facilities storing the largest quantities of hazardous chemicals. We selected 27 facilities that represented various chemical manufacturing industry sectors, such as industrial gases and plastics and resins. We provided this list of facilities to the ACC, which then contacted facility officials and identified 8 facilities willing to host our visits. We visited 6 of these facilities. In addition, we visited another facility that we contacted independently. We recognize that there are risks associated with the transportation sector, but it was not within the scope of our review. We limited our review of security issues to stationary chemical facilities and did not address security concerns surrounding the transportation of hazardous chemicals.[2] In October 2002, we also issued a report on some actions Justice has taken to assess the chemical industry's vulnerabilities to terrorist attack.[3]

Results in Brief

Chemical facilities may be attractive targets for terrorists intent on causing massive damage. The risk of an attack varies among facilities, depending upon several factors, including their location and the types of chemicals they use, store, or manufacture. Many facilities are located in populated areas, where a chemical release could result in injuries or death as well as

[2]We will be reporting on the safety and security of transporting hazardous material by rail in spring 2003.

[3]U.S. General Accounting Office, *Homeland Security: Department of Justice's Response to Its Congressional Mandate to Assess and Report on Chemical Industry Vulnerabilities*, GAO-03-24R, (Washington, D.C.: Oct. 10, 2002).

economic harm. No specific data exist on the actual effects of successful terrorist attacks on chemical facilities. However, according to EPA, 123 chemical facilities located throughout the nation have accidental toxic release "worst-case" scenarios where more than one million people in the surrounding area could be at risk of exposure to a cloud of toxic gas. Approximately 700 facilities could each potentially threaten at least 100,000 people in the surrounding area, and about 3,000 facilities could each potentially threaten at least 10,000 people. To date, no one has comprehensively assessed the security of chemical facilities.

No federal laws explicitly require that chemical facilities assess vulnerabilities or take security actions to safeguard their facilities against terrorist attack. Nevertheless, a number of federal laws impose safety requirements that are applicable to chemical facilities. These requirements do not specifically address security preparedness against terrorism, but they may help mitigate the effects of a chemical release resulting from a terrorist attack. For example, facilities must take safety precautions to detect and minimize the effects of accidental releases, as well as provide prompt emergency response to a release. As part of the safety precautions a facility takes, it might install sensors or sprinklers. While no law explicitly requires facilities to address the threat of terrorism, EPA believes that the Clean Air Act could be interpreted to provide authority to address site security from terrorist attack at chemical facilities. However, EPA has not attempted to use these Clean Air Act provisions. EPA is concerned that such an interpretation would pose significant litigation risk and has concluded that chemical facility security would be more effectively addressed by passage of specific legislation. Currently, EPA is working with chemical industry groups on voluntary initiatives to increase security at their facilities.

The federal government has not comprehensively assessed the chemical industry's vulnerabilities to terrorist attacks. As a result, federal partners—EPA, the Department of Homeland Security, the Department of Justice, and other federal agencies—along with state and local entities, lack comprehensive information on the vulnerabilities the industry faces. However, federal agencies have taken preliminary steps to assist the industry in its preparedness efforts. For example, EPA has issued warning alerts to the industry and informally visited about 30 high-risk facilities to learn about and encourage security efforts. Because industry's efforts are voluntary, however, EPA is not currently monitoring or documenting the extent to which chemical facilities have implemented security measures. The Department of Homeland Security is currently determining how it will implement the National Strategy for Homeland Security, which outlines

the principles and goals for the new department. The specific roles and responsibilities for achieving these goals are still being debated. In May 2002, Justice submitted an interim report to Congress that described observations on security at 11 chemical manufacturing facilities. As we reported in October 2002, however, Justice has not prepared a more comprehensive final report to Congress on the industry's vulnerabilities, which it was required by law to deliver in August 2002.

To its credit, the chemical industry has undertaken a number of initiatives to address security concerns at chemical facilities, including developing security guidelines and tools to assess vulnerabilities, but challenges remain. The American Chemistry Council—whose members own or operate approximately 1,000 (or about 7 percent) of the 15,000 facilities subject to the Clean Air Act's risk management plan provisions—now requires its members to conduct security vulnerability assessments and implement security improvements. Other industry groups that use or store chemicals are also developing security initiatives, but the extent of these efforts varies from issuing security guidance to requiring vulnerability assessments. EPA officials estimate that voluntary initiatives led by industry associations only reach a portion of the 15,000 facilities subject to risk management plan provisions. Moreover, the industry faces a number of challenges in preparing facilities against terrorist attacks, including ensuring that facilities obtain adequate information on threats and determining the appropriate security measures given the level of risk. The industry also faces a challenge in ensuring that all facilities that produce, use, or store hazardous chemicals are addressing security concerns. Despite the voluntary industry initiatives to date, the extent of security preparedness across the chemical industry is unknown. Furthermore, both the Secretary of Homeland Security and the Administrator of EPA have stated that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness. They also stated that they would support bipartisan legislation to require the 15,000 chemical facilities nationwide that contain large quantities of hazardous chemicals to comprehensively assess their vulnerabilities and then act to reduce them.

In light of the challenges facing the industry and the gravity of the potential threat, we recommend that the Secretary of Homeland Security and the Administrator of EPA jointly develop, in consultation with the Office of Homeland Security, a comprehensive national chemical security strategy that is both practical and cost effective. This national strategy should

- identify high-risk facilities based on factors including the level of threat and collect information on industry security preparedness;
- specify the roles and responsibilities of each federal agency partnering with the chemical industry;
- develop appropriate information sharing mechanisms; and
- develop a legislative proposal, in consultation with industry and other appropriate groups, to require these chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action.

We provided a draft of this report to the Departments of Homeland Security and Justice and to EPA for review and comment. These agencies generally agreed with the report's findings and conclusions. EPA also provided a number of technical comments and clarifications, which we incorporated in the report as appropriate. The Department of Homeland Security and EPA agreed that legislation requiring chemical facilities to assess and address vulnerabilities to terrorist attack should be enacted. Both agencies noted that the February 2003 President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets asks the Department of Homeland Security, in concert with the White House, EPA, and other key departments and agencies, to work with Congress to enact legislation requiring certain chemical facilities to perform vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified. We revised our report to include the President's newly released strategy for protecting the chemical industry infrastructure. In responding to our draft, Justice commented that our report failed to state Justice's conclusion that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible. We revised our report to address Justice's comments, and made other revisions as appropriate.

Background

Chemical facilities manufacture a host of products—including basic organic chemicals, plastic materials and resins, petrochemicals, and industrial gases, to name a few. Other facilities, such as fertilizer and pesticide facilities, pulp and paper manufacturers, water facilities, and refineries, also house large quantities of chemicals.

EPA has a role in preventing and mitigating accidental releases at chemical facilities through, among other things, the RMP provisions of the Clean Air Act. Under these provisions, EPA identified 140 toxic and flammable chemicals that, when present above certain threshold amounts, would pose the greatest risk to human health and the environment if

released. According to EPA, approximately 15,000 facilities in a variety of industries produce, use, or store one or more of these chemicals beyond threshold amounts in one or more processes (e.g., single or interconnected vessels or tanks). Table 1 outlines the number and percent of processes in different industry sectors that maintain more than threshold amounts of these hazardous chemicals.

Table 1: Number and Percent of RMP-Covered Processes by Industry Sector

Industry sector	Number of processes	Percent of processes
Agriculture & farming, farm supply, fertilizer production, pesticides	6,317	31%
Water supply and wastewater treatment	3,753	18%
Chemical manufacturing	3,803	18%
Energy production, transmission, transport, and sale	3,038	15%
Food and beverage manufacturing & storage (including refrigerated warehousing)	2,366	11%
Chemical warehousing (not including refrigerated warehousing)	318	2%
Other[a]	1,075	5%
Total[b]	**20,670**	**100%**

Source: EPA.

[a]Other represents a large variety of industry sectors including pulp mills, iron and steel mills, cement manufacturing, and computer manufacturing.

[b]The total number of covered processes is not equal to the 15,000 RMP facilities because some RMP facilities have more than one covered process (i.e., a process containing more than a threshold amount of a covered hazardous chemical).

In July 2002, the President issued the National Strategy for Homeland Security, which spells out the activities that must be accomplished or coordinated to improve the nation's readiness to address terrorism. The strategy designated EPA as the lead agency for interacting with the chemical industry and the hazardous materials sector. Although the strategy outlines a framework for agencies' activities by setting forth overarching goals, the specific roles and responsibilities for achieving these goals are still being debated. In November 2002, Congress created the Department of Homeland Security to consolidate many homeland security activities and coordinate the efforts of federal, state, and local governments and the private sector.

A number of other critical infrastructures have federal security requirements. For example, all commercial nuclear power plants licensed by the Nuclear Regulatory Commission are subject to a number of security requirements, including placing physical barriers outside the operating

reactor area, limiting access to vital areas, maintaining a trained security force, and conducting simulated terrorist attack exercises. Congress passed the Aviation and Transportation Security Act of 2001, which transferred aviation security from the Federal Aviation Administration to the newly created Transportation Security Administration and directed the agency to take over responsibility for airport screening. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires community water systems serving more than 3,300 people to conduct a vulnerability assessment to terrorist attacks, prepare an emergency response plan that incorporates the results of the vulnerability assessment, certify to EPA that the vulnerability assessment and emergency response plan have been completed, and provide a copy of the assessment to EPA. To improve security in our nation's ports, the Maritime Transportation Security Act of 2002 directs the Secretary of the Department of Homeland Security to identify vessels and port facilities that pose a high risk of being involved in a transportation security incident and to conduct a vulnerability assessment of these facilities and vessels.[4]

Congress is considering several legislative proposals that would grant EPA authority to require chemical facilities to take security steps. The 108th Congress has introduced S. 6 and S. 157 that direct EPA, in consultation with the Department of Homeland Security, to identify "high-priority" chemical facilities based on the severity of the threat and require these facilities to identify hazards; perform vulnerability assessments; and develop and implement prevention, preparedness, and response plans to address vulnerabilities and hazards. The facilities would then be required to send these assessments and plans to EPA. EPA and the Department of Homeland Security would jointly review the assessments and plans and certify compliance.

[4]In responding to our draft, EPA noted that approximately 2,000 RMP facilities may be covered under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Regulations under the Maritime Transportation Security Act of 2002 may also cover some RMP facilities.

An Attack Against Chemical Facilities Could Cause Economic Harm and Loss of Life

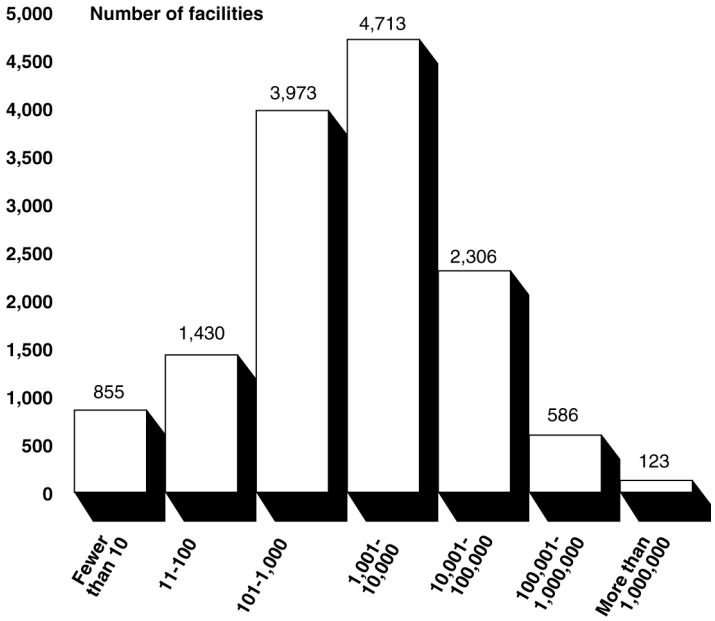
Experts agree that chemical facilities present an attractive target for terrorists intent on causing massive damage because many facilities house toxic chemicals that could become airborne and drift to surrounding areas if released. Alternatively, terrorists could steal chemicals, which could be used to create a weapon capable of causing harm. Justice has been warning of the terrorist threat to chemical facilities for a number of years and has concluded that the risk of an attempt in the foreseeable future to cause an industrial chemical release is both real and credible. In fact, according to Justice, domestic terrorists plotted to use a destructive device against a U.S. facility that housed millions of gallons of propane in the late 1990s. In testimony on February 6, 2002, the Director of the Central Intelligence Agency warned of the potential for an attack by al Qaeda on chemical facilities.

Some chemical facilities may be at higher risk of a terrorist attack than others when they contain large amounts of toxic chemicals and are located near population centers assuming that the objective is a catastrophic release. Attacks on such facilities could harm a large number of people, with health effects ranging from mild irritation to death, cause large-scale evacuations, and disrupt the local or regional economy. No specific data are available on what the actual effects of successful terrorist attacks on chemical facilities would be. However, facilities subject to the RMP provisions submit to EPA estimates of the potential consequences to surrounding communities of hypothetical accidental "worst-case" chemical releases from their plants. These estimates include the residential population located within the range of a toxic gas cloud produced by a "worst-case" chemical release, called the "vulnerable zone." According to EPA, 123 chemical facilities located throughout the nation have toxic "worst-case" scenarios where more than one million people would be in the "vulnerable zone" and could be at risk of exposure to a cloud of toxic gas.[5] About 600 facilities could each potentially threaten

[5]"Vulnerable zones" are determined by drawing a circle around a facility with the radius of the circle equal to the distance a toxic gas cloud would travel before dissipating to relatively harmless levels. Because, in an actual event, the toxic cloud would only cover a fraction of that circle, it is unlikely that the event would actually result in exposure of the entire population estimated in the "worst-case" scenario, according to EPA. The number of persons within a "vulnerable zone" is larger than the number of persons that would be affected by a "worst-case" scenario. In addition, EPA's requirements for "worst-case" release analysis tend to result in consequence estimates that are significantly higher than what is likely to actually occur. For example, "worst-case" release analysis does not take into account active mitigation measures facilities often employ to reduce the consequences of releases.

between 100,000 and a million people, and about 2,300 facilities could each potentially threaten between 10,000 and 100,000 people within these facilities' "vulnerable zones." Figure 1 shows the residential population within the "vulnerable zone" that could potentially be threatened by an accidental toxic chemical release from a U.S. facility under a "worst-case" scenario.

Figure 1: Number of Facilities with Worst-Case Accidental Release Scenarios by Residential Population Potentially Threatened



Source: EPA.

Notes: EPA, *Chemical Accident Risks in U.S. Industry – A Preliminary Analysis of Accident Risk Data from U.S. Hazardous Chemical Facilities*, Washington, D.C.: September 25, 2000.

This figure includes only those facilities with toxic chemicals that could lead to a "worst-case" scenario. Facilities that only have flammable chemical "worst-case" scenarios are not included. Flammable chemicals affect fewer people because the distance the flammable substance travels tends to be significantly shorter.

According to EPA, "worst-case" scenarios do not consider the potential causes of a release or how different causes or other circumstances, such as safety features, could lessen the consequences of a release. Hence, the "worst-case" scenario calculations would be overstating the potential consequences. However, the RMP regulation requires facilities to estimate the effects of a toxic chemical release involving the greatest amount of the toxic chemical held in a single vessel or pipe—not the entire quantity on site. Therefore, for some facilities it is conceivable that an attack, where

multiple chemical vessels were breached simultaneously, could result in an even larger release, involving more severe potential consequences, than those estimated in the RMP "worst-case" scenarios. Other factors could also make a facility a more attractive target. For example, a facility that is widely recognizable, located near a historic or iconic symbol, or critical to supporting other infrastructures could be at higher risk.

The Army has also estimated high potential damage to the population from a toxic chemical release. During a 2001 informal meeting with a number of agencies, the Army Office of The Surgeon General proposed, based on generic estimates, that it was conceivable that as many as 2.4 million people could request medical treatment if a terrorist caused a release of a toxic chemical.[6] According to officials from that office, these estimates include anyone who seeks medical attention as a result of the release—including people with minor irritations or concerns. Finally, a 2002 Brookings Institution report ranks an attack on toxic chemical plants behind only biological and atomic attacks in terms of possible fatalities.[7]

Currently, no one has comprehensively assessed security across the nation at facilities that house chemicals. According to a 1999 study by the Agency for Toxic Substances and Disease Registry (ATSDR), security at chemical plants in two communities was fair to very poor. ATSDR observed security vulnerabilities such as freely accessible chemical barge terminals and chemical rail cars parked near residential areas in communities where plants are located. Furthermore, during a limited review of chemical industry vulnerabilities conducted primarily before September 11, 2001, Justice found that security at 11 chemical facilities was comparable to security found at other industrial facilities. According to Justice, some facilities may need to implement more effective security systems and develop alternative means to reduce the potential consequences of a successful attack. The effectiveness of security at some facilities may also be in doubt as evidenced by several media accounts of reporters and environmental activists gaining access to chemical tanks and computer centers that control manufacturing processes at these facilities.

[6]U.S. Army, *Draft Medical NBC Hazard Analysis of Chemical-Biological-Radiological-Nuclear-High Explosive Threat, Possible Scenarios & Planning Requirements*, Army Office of the Surgeon General (October 2001).

[7]The Brookings Institution, *Protecting the American Homeland: A Preliminary Analysis*, (Washington, D.C.: 2002).

No Federal Requirements Specifically Require Chemical Facilities to Address the Threat of Terrorism

No federal laws explicitly require that chemical facilities take security actions to safeguard their facilities against a terrorist attack. A number of federal laws impose safety requirements applicable to chemical facilities, but these requirements do not specifically address security preparedness against terrorism. However, these safety requirements may help mitigate the effects of such an attack. While no law explicitly requires facilities to address the threat of terrorism, EPA believes that the Clean Air Act could be interpreted to provide authority to address site security from terrorist attack at chemical facilities. However, EPA has not attempted to use these Clean Air Act provisions. EPA is concerned that such an interpretation would pose significant litigation risk and has concluded that chemical facility security would be more effectively addressed by passage of specific legislation. Currently, EPA is working with chemical industry groups on voluntary initiatives to increase security at their facilities.

Federal Government Does Not Specifically Require Chemical Facilities to Address the Threat of Terrorism, but It Has Requirements Addressing Safety and Emergency Response

While the federal government does not require chemical facilities to take security measures to protect against a terrorist attack, it does require certain facilities to take security precautions directed to prevent trespassing or theft. However, these requirements do not cover a wide range of chemical facilities and may do little to actually prevent a terrorist attack. For example, under EPA's regulations implementing the Resource Conservation and Recovery Act of 1976, facilities that house hazardous waste generally must take certain security actions, such as posting warning signs and using a 24-hour surveillance system or surrounding the active portion of the facility with a barrier and controlled entry gates.[8] However, according to EPA, these requirements would be applicable to only approximately 21 percent of the 15,000 RMP facilities because this 21 percent is also subject to the Resource Conservation and Recovery Act's requirements. Moreover, while a facility's use of a 24-hour surveillance system or a means to control entry may help impede a terrorist's access to a facility, these security measures are aimed at

[8] 40 C.F.R. § 264.14.

keeping out trespassers or wanderers, not intentional intruders, according to EPA.[9]

Several statutes, including the Occupational Safety and Health Act, the Clean Air Act, and the Emergency Planning and Community Right-to-Know Act, impose safety and emergency response requirements on chemical facilities that may incidentally reduce the likelihood and mitigate the consequences of terrorist attacks.[10] The Occupational Safety and Health Act imposes a number of safety requirements, including a general duty to furnish a workplace free from recognized hazards that may cause death or serious physical harm to employees.[11] The 1990 amendments to the Clean Air Act also include safety requirements, including a general duty to prevent and mitigate accidental chemical releases. Specifically, section 112(r) of the Clean Air Act includes a general duty clause directing owners and operators of facilities that produce, use, handle, or store listed or other extremely hazardous substances to identify hazards, design and maintain a safe facility to prevent releases, and minimize the consequences of any accidental releases that occur.[12]

Section 112(r) also directs EPA to establish regulations under which owners and operators of facilities that handle listed (or "regulated") extremely hazardous substances over a threshold amount are required to prepare and implement a risk management plan to detect and prevent or minimize accidental releases.[13] Facility owners and operators must conduct a hazard assessment that includes an evaluation of worst-case accidental release scenarios. They must also implement a program to

[9]In addition, the Drug Enforcement Agency (DEA) requires any chemical facility that manufactures one of the 32 chemicals that can be used as a precursor to illegal drugs or controlled substances to securely store, restrict access, and monitor inventories of these chemicals. However, according to EPA, these DEA security requirements are only applicable to a few chemicals that when accidentally or intentionally released could cause harm to humans or the environment. Sixty-two of the 15,000 RMP facilities have these chemicals.

[10]We focus our discussion in this report on those requirements dealing with assessments of hazards and emergency response. However, the Toxic Substances Control Act also may mitigate the consequences of a terrorist attack by limiting or eliminating certain toxic chemicals that a facility manufactures or uses.

[11]See 29 U.S.C. § 654 (a)(1).

[12]See 42 U.S.C. § 7412 (r)(1).

[13]See 42 U.S.C. § 7412 (r)(7). Regulated substances include 77 toxic substances, such as ammonia and chlorine, and 63 flammable substances, such as butane and hydrogen.

prevent accidental releases that includes safety precautions and maintenance, monitoring, and training measures, and have an emergency response plan with specific actions to be taken in response to an accidental release. In addition, these facilities must coordinate their activities with community emergency response organizations. Facility owners or operators must generally discuss these activities in an RMP and submit it to EPA.

The Clean Air Act Amendments of 1990 also call for OSHA to establish a standard to protect employees from hazards associated with accidental releases of highly hazardous chemicals in the workplace.[14] OSHA's process safety management standard (on which EPA's RMP regulations are modeled) requires facilities to assess and address the hazards of their chemical process. Implementation of the standard makes facilities safer and could help mitigate the consequences of a terrorist attack. Regulated companies in over 95 different industry sectors, including chemical manufacturing, must conduct hazard evaluations, known as process hazard analyses, for every step of a covered manufacturing process.[15] These analyses must include hazards of the process, engineering and administrative controls applicable to the hazards, facilities siting, and evaluation of the range of possible health and safety effects of failures of controls on employees. Based on these analyses, employers must take action to address the findings. Examples of measures that facilities could take include storing smaller amounts of chemicals, substituting less dangerous chemicals for chemicals currently in use, installing automatic shutdown systems, and installing pipes and other critical equipment that are stronger and better-shielded.

The Emergency Planning and Community Right-to-Know Act focuses on understanding hazards and planning for emergencies to ensure that if a release occurs, local responders will be able to take quick, effective actions to protect public health and the environment.[16] Under this act, owners of facilities that maintain specified quantities of certain extremely hazardous chemicals must submit information annually on their chemical

[14]P.L 101-549, § 304(a). See 29 C.F.R. Part 1910.

[15]The process safety management standard applies to processes that contain at least a threshold quantity of a toxic or reactive highly hazardous chemical, as specified in an appendix to the standard. The standard also applies to facilities that use or store 10,000 pounds or greater amounts of flammable liquids and gases.

[16]See 42 U.S.C. § 11001.

inventory to state and local emergency response officials.[17] The act also requires that each state establish a State Emergency Response Commission to oversee local emergency planning and create local emergency planning committees. Local emergency planning committee members include local police, fire fighters, health officials, representatives from government and media, community groups, and representatives from facilities. These committees must develop and periodically review their communities' emergency response plans, including the identification of chemical facilities, and outline procedures for response personnel to follow in the event of a chemical incident.

All of these requirements could potentially mitigate a terrorist attack in a number of ways. First, because some of these requirements only apply to facilities with more than threshold quantities of certain chemicals, facility owners have an incentive to reduce or eliminate these chemicals, which may make the facility a less attractive target or minimize the impact of an attack. Second, both the RMP and process safety management hazard analyses require operators to identify the areas of their plants that are vulnerable to a chemical release. When facilities implement measures to improve the safety of these areas, such as installing sensors and sprinklers, the impact of a terrorist-caused release may be lessened. Third, the emergency response plans increase preparedness for a chemical release—whether intentional or unintentional. More coordinated and immediate emergency response could mitigate the consequences of a terrorist attack.

In addition to these federal safety requirements, some states and localities have imposed additional safety requirements on chemical facilities and, in some instances, have addressed the security of chemical facilities from terrorism. For example, Contra Costa County, California, in implementing EPA's RMP provisions, requires that chemical facilities incorporate inherently safer technologies. Specifically dealing with the threat of terrorism, New Jersey has implemented criminal penalties for any toxic chemical manufacturer who recklessly allows an unauthorized individual to obtain access to the chemical. In addition, Baltimore, Maryland, passed a city ordinance addressing the threat of terrorism that requires chemical

[17]The information to be provided includes (1) an estimated range of the maximum amount of specified hazardous chemicals present at the facility at any time during the preceding calendar year, (2) an estimated range of the average amount of these chemicals present daily, and (3) the location in the facility of the specified chemicals. Inventory forms are required for approximately 500,000 materials.

manufacturers to follow a set of safety and security regulations devised by its fire and police commissioners. Companies that fail to comply with the ordinance may face penalties such as the withholding or suspension of facility operating permits.

EPA's Views of Its Authority to Require Chemical Facilities to Prepare for Terrorist Acts

EPA believes that the Clean Air Act could be interpreted to provide authority to address site security from terrorist attack at chemical facilities. However, EPA has not attempted to use these Clean Air Act provisions. EPA is concerned that such an interpretation would pose significant litigation risk and has concluded that chemical facility security would be more effectively addressed by passage of specific legislation. We find that EPA could reasonably interpret its Clean Air Act authority to cover chemical security, but also agree with the agency that this interpretation could be open to challenges.

Section 112(r) of the Clean Air Act—added by the Clean Air Act Amendments of 1990—imposes certain requirements on chemical facilities with regard to "accidental releases." The act defines an accidental release as an unanticipated emission of a regulated substance or other extremely hazardous substance into the air. Arguably, any chemical release caused by a terrorist attack would be unanticipated and thus could be covered under the Clean Air Act. An interpretation of an unanticipated emission as including an emission due to a terrorist attack would provide EPA with authority under Section 112(r)'s RMP provisions and the general duty clause to require security measures or vulnerability assessments with regard to terrorism.

The Clean Air Act's RMP provisions could be interpreted to provide EPA authority to require facilities to take actions to improve their security. Under the RMP provisions, owners and operators of facilities producing, processing, handling, or storing more than a threshold quantity of a regulated chemical must detect and prevent or minimize "accidental releases" and provide prompt emergency response to a release to protect human health and the environment. For example, EPA could require facilities to include security vulnerability assessments as part of their RMP hazard assessments, identifying the potential public exposure that could result from a terrorist attack and incorporating the threat of terrorism into the "worst-case" release scenario. However, current EPA regulations do not require facilities to assess their vulnerability to terrorist attack as part of their RMP. EPA would need to revise its regulations to require that facilities take the threat of terrorism into account.

EPA could also interpret the Clean Air Act's general duty clause to address chemical facility security from terrorism. The general duty clause requires owners and operators of stationary sources producing, processing, handling, or storing listed or other extremely hazardous substances to (1) identify hazards that may result from releases using appropriate hazard assessment techniques; (2) design and maintain a safe facility, taking the steps necessary to prevent releases; and (3) minimize the consequences of accidental releases that do occur. According to EPA, it would not have to make any regulatory changes as it currently implements the general duty clause through guidance. Thus, EPA could revise its existing guidance or issue new guidance to include managing the risk of terrorism as within owners and operators' responsibility under the general duty clause. Second, the clause covers not only the specific chemicals listed under the RMP regulations, but also any other extremely hazardous chemicals. The Clean Air Act does not define an extremely hazardous chemical, and EPA interprets this term broadly. In addition, unlike the RMP provisions, the general duty clause is not limited to facilities that have more than a threshold amount of an extremely hazardous chemical. Thus, facilities that are not covered under the RMP provisions because their chemical amounts are below the threshold amount are covered under the general duty clause. However, if EPA chose to use the general duty clause to address threats to facilities from terrorism, it would face some limitations. Facility owners and operators must demonstrate safe practices at their facilities, but there are no specific standards that facilities have to meet. Since the general duty clause is not implemented by regulations, there are no EPA standards specifically defining the duty. Instead, EPA generally looks to industry and other standards to indicate what facilities should do to prevent and mitigate accidental releases. With respect to chemical facility security against terrorism, according to EPA, there are few such standards.

While EPA believes that the Clean Air Act could be interpreted to authorize EPA to require chemical plants to address security against terrorism, there are a number of practical and legal arguments against this interpretation. First, a release due to a terrorist attack is not entirely unanticipated, as it is an intentional act. Second, a potential argument against EPA using its general duty clause to require facilities to address the threat of terrorism is the relationship between EPA's general duty clause and OSHA's general duty clause. Clean Air Act section 112(r) provides that chemical facility owners and operators have a "general duty in the same manner and to the same extent" as OSHA's general duty clause. However, the Department of Labor informed us that it does not believe OSHA's general duty clause provides it with authority to address

the threat of terrorism.[18] In responding to our draft, Justice expressed concerns that the Clean Air Act does not provide sufficient protection against dissemination of sensitive information that could be used by terrorists.

In light of the litigation risk and the importance of an effective response to the chemical security issue, EPA has decided not to attempt to require vulnerability assessments or security enhancements under the Clean Air Act. EPA has concluded that chemical facility security would be more effectively addressed by passage of specific legislation. Currently, EPA is working with the chemical industry to promote security enhancements.

Federal Agencies Have Not Comprehensively Assessed the Vulnerability of the Chemical Industry to Terrorism, but Have Taken Some Preliminary Steps

The federal government lacks comprehensive information on the chemical industry's vulnerabilities to terrorist attacks because it has not comprehensively assessed the industry. However, federal agencies have taken preliminary steps to assist the industry in its preparedness efforts. For example, EPA has issued warning alerts to the industry and informally visited about 30 high-risk facilities to learn about and encourage security efforts. Neither EPA nor any other federal entity is currently monitoring or documenting the extent to which the industry has implemented security measures. In addition, the Department of Homeland Security is currently determining how it will implement the National Strategy for Homeland Security. Finally, in May 2002, Justice submitted an interim report to Congress that described observations on security at 11 chemical manufacturing facilities. However, as we reported in October 2002, Justice has not prepared a more comprehensive final report to Congress on the industry's vulnerabilities, which it was required by law to deliver in August 2002.

EPA Has Developed a Strategy and Is Supporting Industry's Voluntary Security Initiatives

EPA has not been called upon to comprehensively assess the vulnerability of the chemical industry to terrorism but has conducted some limited analysis of RMP facilities. For example, EPA officials conducted a preliminary analysis of their database of RMP facilities to identify high-risk sites for the Office of Homeland Security (OHS) and FBI. But these

[18]According to EPA, the legislative history of the Clean Air Act's "same extent, same manner" provision suggests that Congress intended only to adopt the four-part test for establishing a violation of the general duty that had been set forth in the OSHA *Duriron* case. See *Occupational Safety and Health Review Commission v. Duriron Co.*, 11 O.S.H. Cas. (BNA) 1405 (1983).

facilities are only a portion of the universe of all industrial facilities that house toxic or hazardous chemicals. While RMP facilities pose the greatest danger of harm to the surrounding community in the event of a catastrophic release, non-RMP facilities may also house dangerous chemicals that could harm the surrounding population or be stolen to use in a terrorist attack. EPA has not analyzed non-RMP facilities to determine whether any of those facilities should be considered at high risk for a terrorist attack.

EPA has assisted industry security efforts in the following ways:

- In February 2000, EPA issued guidance to the industry to increase awareness of the possible hazards of terrorist attacks. The guidance included common security measures for companies to consider and sources of information to assist with security. Since September 11, 2001, EPA has also issued security advisories to several chemical industry sectors, reminding them to be vigilant regarding the physical security of chemicals.
- In 2001, EPA advised a number of industry organizations regarding the development of security guidelines and supported the development by Justice and industry of methodologies for assessing vulnerabilities.
- In 2001 and 2002, EPA, along with trade associations, sponsored a series of regional meetings to share information on chemical security.
- In 2002, EPA hosted seven training classes nationwide on the application of vulnerability assessment methodologies; these classes were attended by industry, federal, state, and local officials.
- EPA is collecting e-mail addresses for RMP facilities to share threat or hazard alert information quickly. EPA may also use the e-mail system to outreach to facilities for guidance and best practices.
- EPA officials are incorporating informal discussions about security issues during their visits to facilities for other programs, such as RMP and the Emergency Planning and Community Right-to-Know Act. For example, EPA Region VII, which is responsible for four midwestern states, discussed security issues during visits to approximately 40 facilities in 2002.

Based on its analysis of RMP facilities, EPA visited 30 high-risk chemical facilities specifically to discuss security issues. According to EPA officials, these visits were designed to help the agency better understand the facilities' current and planned security efforts and provide an opportunity to share suggestions for information tools that facilities can use to assess and address security vulnerabilities. In early 2003, EPA briefed the Administrator and OHS on these visits. EPA officials said that these visits

were not part of any enforcement or regulatory action, and meeting with the EPA staff was at the discretion of the facility.

According to EPA officials, the agency developed a number of draft principles for chemical facilities, such as requiring high-risk facilities to conduct vulnerability assessments. These principles were discussed with an interagency task force that included the Office of Homeland Security. The group decided to pursue specific chemical security legislation and is fostering voluntary security improvements at chemical facilities. Furthermore, in September 2002, EPA issued a Strategic Plan for Homeland Security that describes its goal of supporting the chemical industry in assessing and reducing vulnerabilities and strengthening detection and response capabilities. EPA plans to work with the industry on voluntary initiatives but has no plans to monitor or document the extent to which the industry has implemented voluntary security measures. EPA's plans to accomplish this goal include

- assisting industry in developing vulnerability assessment guidance, identifying potential security enhancements, examining the feasibility of integrating inherently safer technologies, and exploring the use of third-party verification for security at chemical facilities;
- identifying site security concerns for small businesses and providing outreach materials and technical assistance to these facilities; and
- working with emergency planning organizations to assist them in understanding site security hazards and prioritizing risks at chemical facilities.

The Office of Homeland Security Has Played a Coordinating Role

The President's Office of Homeland Security coordinated with other federal agencies and worked with industry to address chemical security concerns. OHS formed an interagency group, including EPA, OSHA, the Department of Energy, and the Coast Guard, to discuss issues critical to the chemical industry. OHS and EPA hosted a workshop attended by both government and private sector officials to identify solutions to vulnerabilities in the nation's chemical infrastructure. OHS is compiling information gathered from this workshop and those for other critical industry sectors to report on critical infrastructure protection. Since its creation in November 2002, the Department of Homeland Security has been determining how it will implement the principles and goals outlined in the Office of Homeland Security's national strategy. In February 2003, the Office of Homeland Security issued the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, which further defines the goals and objectives to secure infrastructures. The

strategy directs the Department of Homeland Security, in concert with the White House, EPA, and other key departments and agencies, to work with Congress to enact legislation to help protect the American public by requiring certain chemical facilities, particularly those that maintain large quantities of hazardous chemicals near population centers, to perform vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified.

Justice Initiated Actions to Study the Vulnerability of the Chemical Industry but Has Not Fully Met Its Statutory Requirements

Justice has only partially fulfilled its mandate to review and report on the vulnerability of chemical facilities to terrorist or criminal attack. The Chemical Safety Information, Site Security and Fuels Regulatory Relief Act of 1999 required Justice to conduct this review and prepare two reports—an interim report containing preliminary findings by August 5, 2000, and a final report by August 5, 2002. Justice prepared and submitted an interim report to Congress in May 2002, nearly 2 years after it was due, and has not submitted its final report to Congress. The interim report was based on observations made at 11 chemical manufacturing facilities Justice visited to develop a methodology for assessing vulnerability. While the interim report contains the elements required by the act, the results cannot be generalized to the industry as a whole. In its fiscal year 2003 budget, Justice asked for $3 million to conduct chemical plant vulnerability assessments. In the February 2003 Conference report[19] on Justice's appropriation act for fiscal year 2003, Congress directed that $3 million of the funding being transferred to the Department of Homeland Security from Justice's general administration account be used for the chemical plant vulnerability assessments. Justice believes that chemical plant vulnerability assessments are now part of the mission of the Department of Homeland Security.

While Justice has not assessed the vulnerability of the chemical industry, it has provided the industry with a tool for individual facilities to use in assessing their vulnerabilities. Justice, together with the Department of Energy's Sandia National Laboratories, developed a vulnerability assessment methodology for evaluating the vulnerability to terrorist attack of facilities handling chemicals. In July 2002, Justice made the methodology publicly available for chemical companies to use in identifying and assessing their threats, risks, and vulnerabilities. The

[19]H.R. Conf. Rept. No. 108-10, at 600 (2003).

methodology also helps facilities develop recommendations to reduce risk, where appropriate. The steps in the methodology include

- assessing the type, nature, and physical characteristics of chemicals, as well as a facility's operational practices and security systems;
- evaluating the consequences if a facility is targeted;
- determining the attributes of the most likely threats (e.g., insiders, activists, terrorists);
- evaluating the effectiveness of current security measures against various threats;
- quantifying the risk as a function of the likelihood of attack, security effectiveness, and consequences; and
- conducting a cost-benefit analysis of possible security upgrades.

Justice's FBI is the lead federal agency for the operational response to terrorism, responsible for weapons of mass destruction threat assessment and communicating warnings. The FBI's National Infrastructure Protection Center collects information from the U.S. intelligence community, the FBI's criminal investigations, other federal agencies, and the private sector. If a threat involving chemical, biological, nuclear, or radiological materials surfaces, subject matter experts in various units within the agency assess the credibility of the threat. As a result of this analysis, the FBI uses an array of mechanisms to issue and disseminate warnings to appropriate entities in the federal government and the private sector so that they can take immediate protective steps.

Working with ACC, an industry association representing chemical manufacturers, the FBI created the Chemical Sector Information Sharing and Analysis Center to collect and share threat information for the chemical industry.[20] This center, which began operation in April 2002, provides a mechanism for companies to report unexplained or suspicious incidents involving chemical facilities or chemicals in commerce directly to the FBI. Likewise, the FBI can quickly exchange critical threat and incident information with the chemical industry. To operate the center, ACC uses its existing 24-hour communication network for sharing information about chemical emergencies. Any company, not just ACC members, engaged in the production, storage, transportation, sale, or delivery of chemicals may participate.

[20]Presidential Decision Directive 63 required Justice to develop Information Sharing and Analysis Centers for eight critical infrastructures. The chemical infrastructure was not part of this initial directive, but the government has expanded the number of such sectors.

Finally, agents in the FBI's local field offices provide information and technical assistance to state and local jurisdictions and to some chemical facilities to bolster their preparedness to respond to terrorist incidents. The FBI has contacted chemical facilities and distributed Chemical Outreach booklets to chemical suppliers and manufacturers with information relevant to identifying suspicious purchases, materials, or precursors that may be used as weapons of mass destruction by terrorists, as well as contact information for reporting suspicious activity.

Chemical Industry Has Taken Actions to Address Security Concerns, but Faces Significant Challenges in Preparing Against Terrorist Attacks

The chemical manufacturing industry has undertaken a number of initiatives to address security concerns at chemical facilities, including developing security guidelines and tools to assess vulnerabilities, but challenges remain. The ACC requires its members to conduct security vulnerability assessments and implement security improvements. Other industry groups are also developing security initiatives, but the extent of these efforts varies from issuing security guidance to requiring vulnerability assessments. Moreover, the industry faces a number of challenges in preparing facilities against terrorist attacks, including ensuring that facilities obtain adequate information on threats and determining the appropriate security measures given the level of risk. Despite the voluntary industry initiatives to date, the extent of security preparedness across the chemical industry is unknown. While the Secretary of Homeland Security and the Administrator of EPA commended the industry's voluntary efforts to reduce the vulnerability of U.S. chemical facilities to terrorist attacks, they stated that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness. They also stated they would support bipartisan legislation to require the 15,000 chemical facilities nationwide that contain large quantities of hazardous chemicals to comprehensively assess their vulnerabilities and then act to reduce them.

Chemical Industry Has Undertaken a Number of Voluntary Initiatives to Address Security

In response to increased security concerns after the terrorist attacks of September 11, 2001, chemical industry groups have undertaken a number of security initiatives, including the development of security guidance and assessment tools. All of the industry groups with whom we met have taken actions such as forming security task forces, holding meetings and conferences to share security information with members, and participating in security briefings with federal agencies. In October 2001, ACC, the Chlorine Institute, Inc., and the Synthetic Organic Chemical Manufacturers Association (SOCMA) released guidelines developed by industry process safety and security experts that outline elements of security programs and

suggest security practices that chemical plant managers can tailor to their facilities' needs.[21] The guidelines address security at fixed facilities and are intended to assist facility managers in determining appropriate security measures commensurate with a facility's level of risk. ACC also worked with EPA, FBI, and others to organize regional security briefings around the nation.

In addition to Justice's methodology to assess chemical facilities' vulnerabilities, industry groups developed tools for chemical facility managers to utilize in assessing their security vulnerabilities and risks. The Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers, a research institution that promotes safety at chemical facilities, developed a security vulnerability analysis that chemical facilities can use to evaluate their risks and focus efforts on hazardous chemical processes and sites where the severity of the attack would be the greatest and the difficulty of attack would be the least. CCPS has also formed a security vulnerability assessment users group to share experiences and to learn from each other on the use of the methodology. SOCMA tailored its vulnerability assessment model to the needs of smaller facilities that manufacture a variety of chemicals in batches, rather than those that continuously manufacture a single product.

Industry groups have also spearheaded efforts to address cyber-security concerns. Attacks on computer systems that control chemical facility operations pose a serious threat. Cyber-security is necessary to protect critical information systems from loss, theft, or damage, as well as to protect chemical processes from hazardous disruptions and unwanted chemical releases. Working with the President's Critical Infrastructure Protection Board, a group of industry representatives—with expertise in information security, the security of computers that control chemical processes, and physical security—crafted a national chemicals sector cyber-security strategy to improve the security of industry information and information infrastructure. The chemical sectors cyber-security strategy is part of the President's National Strategy to Secure Cyberspace, which outlines specific strategies for critical infrastructures.

[21]The Chlorine Institute, Inc., represents companies that are involved in the production, distribution, or use of chlorine. SOCMA represents manufacturers who produce specialty chemicals at small- to medium-sized facilities.

In addition to security initiatives, the industry's voluntary safety standards could also potentially help lessen the impact of a terrorist action at a facility. For example, the CCPS has published numerous process safety guidelines aimed at reducing hazards.

Chemical Manufacturers' Industry Association Requires Members to Assess Vulnerabilities and Enhance Security

In response to the terrorist attacks on September 11, 2001, ACC—whose members own or operate approximately 1,000 facilities that are required to submit RMPs—-now requires its members to identify, assess, and address vulnerabilities. Companies must first rank their facilities according to risk to determine the time frame for conducting vulnerability assessments and making security enhancements. To rank facilities, companies use an ACC screening tool to evaluate the difficulty of attack given existing security, the severity of consequences of a successful attack on the surrounding population, and the attractiveness of the target, according to factors such as impact on the economy and disruption to other critical infrastructures. ACC reports that all member companies completed the ranking process by June 2002.

Facility operators then apply a vulnerability assessment methodology to assess potential security risks. Companies may use the Justice vulnerability assessment methodology developed with Sandia National Laboratories, the CCPS methodology, or an equivalent methodology approved by the center. About half a dozen companies have developed methodologies that meet the center's criteria and are tailored to the needs of companies' facilities. Justice's and CCPS's methodologies lead facilities through a multistep process that includes: (1) evaluating on-site chemical hazards, existing safety and security features, and the attractiveness of the facility as a terrorist target; (2) using hypothetical threat scenarios to identify how a facility is vulnerable to attack; and (3) identifying security measures that create layers of protection around a facility's most vulnerable areas to detect, delay, or mitigate the consequences of an attack. Using the companies' rankings for their facilities, ACC established time frames for completing the vulnerability assessment and implementing security measures. The highest-risk ACC member facilities that must submit RMPs are required to complete the process by December 2003.

Once facilities have made the necessary security improvements identified by their vulnerability assessment, ACC's security code generally requires that third parties, such as insurance representatives, local emergency

responders, or local law enforcement officials, verify that these improvements were implemented.[22] The code does not require, however, that third parties verify that the vulnerability assessment is conducted appropriately or that the actions taken by the facility adequately address security risks.

The ACC chemical facilities we visited were progressing on schedule with implementation of ACC's security code. All of these facilities completed the prioritization screening assessment on schedule, and several had identified a team of security and process safety experts to conduct the vulnerability assessment. Facilities are not waiting until they complete their vulnerability assessments to make security improvements. We observed that facilities have implemented a range of security measures since September 11, 2001. These measures include installing perimeter fencing, adding or upgrading security cameras, increasing security guards on site, adding or increasing vehicle inspections, and adding or improving access control systems to restrict access to key areas. Facilities were also planning additional security improvements, such as increasing security training and drills and working to ensure that background checks are conducted for contract personnel.

ACC has made efforts to enlist facilities beyond its membership in voluntary security initiatives. ACC hopes that other chemical industry organizations and groups that handle, transport, and store chemicals will also adopt its security requirements, which are set forth in its Responsible Care security code. According to ACC, through its Responsible Care Partner Program, almost 90 partner companies, primarily transportation companies, agree to implement and report on Responsible Care codes. In addition, associations that represent other industries agree to promote Responsible Care codes to their members. One group, SOCMA, adopted the Responsible Care security code for its member facilities as a condition of membership. However, the extent to which all partner companies and associations implement the codes is unclear.

Although implementation of Responsible Care is a condition of ACC membership, ACC lacks an enforcement mechanism to ensure that member companies comply. ACC stated that facilities must submit

[22]The lowest-risk facilities may use a less rigorous methodology to identify and make security enhancements and are not required to obtain third-party verification that improvements have been made.

periodic updates on their implementation of Responsible Care codes, but ACC does not verify implementation or evaluate the adequacy of facility measures. ACC officials stated that as of April 2002 they had not expelled any member companies for failure to comply with the Responsible Care initiatives. Beginning in 2004, ACC will publicly report the percentage of member company facilities that have completed security vulnerability assessments and third-party verification that security enhancements are implemented, in keeping with the Responsible Care security code time frames. By December 2005, member company headquarters will be required to have implementation of Responsible Care requirements certified by independent third-party auditors.

Other Facilities House Hazardous Chemicals, but Participation in Voluntary Initiatives Is Unclear

While ACC's efforts are commendable, its member facilities comprise only about 7 percent of the facilities required to submit risk management plans to EPA. About 14,000 other facilities manufacture, produce, use, or store chemicals in quantities that require compliance with EPA's RMP program. According to an EPA official, RMP data show that the largest quantities of the most dangerous chemicals are located at facilities that use chemicals, not at facilities that manufacture chemicals. These facilities include agricultural suppliers, such as fertilizer facilities; petroleum and natural gas facilities; food storage facilities; water treatment facilities; and wastewater treatment facilities, among others. In addition, other facilities that house hazardous chemicals listed under the RMP regulations are not subject to RMP requirements because the quantities are below threshold amounts. These facilities could potentially be at risk of terrorist attacks.

Some of these other facilities also have security initiatives underway. For example:

- The Fertilizer Institute, which represents fertilizer manufacturers as well as fertilizer retail and distribution facilities, developed a security code modeled after ACC's code. The code encourages facilities to develop vulnerability assessments and implement a plan based on the assessments. In addition, a security vulnerability methodology for agricultural retail facilities will be developed to assist this sector of the fertilizer industry.
- The American Petroleum Institute, which represents petroleum and natural gas facilities, published security guidelines developed in collaboration with the Department of Energy that are tailored to the differing security needs of industry sectors, such as oil and gas exploration, refining, transportation, and distribution.
- The International Institute of Ammonia Refrigeration, which represents facilities such as food storage warehouses that use ammonia refrigeration,

developed site security guidelines and provided information about security resources to its member facilities.

- The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires, among other things, that all community water systems serving more than 3,300 customers certify to EPA that they have conducted an assessment of vulnerabilities to terrorist attacks. According to EPA, about 2,000 of these community water systems are also RMP facilities.

Despite industry associations' efforts to encourage security actions at facilities, the extent of participation in voluntary initiatives is unclear. EPA officials estimate that voluntary initiatives led by industry associations only reach a portion of the 15,000 RMP facilities. Furthermore, EPA officials stated that these voluntary initiatives raise an issue of accountability, since the extent that industry group members are implementing voluntary initiatives is unknown.

Industry Faces Challenges in Improving Preparedness

Even with the actions the chemical industry has taken to date to address security, it still faces significant preparedness challenges. Trade association and industry officials identified a number of concerns about preparing against terrorist attacks. First, industry officials noted that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information. They stated that chemical companies do not receive enough specific threat information and frequently receive threat information from multiple government agencies. Similarly, in developing its vulnerability assessment methodology, Justice observed that chemical facilities need more specific information about potential threats in order to design their security systems and protocols. Industry officials also noted that efforts to share threat information among industry and federal agencies will be effective only if government agencies provide specific and accurate threat information. Threat information also forms the foundation for some of the tools available to industry to assess facility vulnerabilities. The Justice vulnerability assessment methodology requires threat information as the foundation for hypothesizing about threat scenarios, which form the basis for determining site vulnerabilities.

Second, according to industry officials, chemical companies face a challenge in achieving cost-effective security solutions, noting that companies must weigh the cost of implementing countermeasures against the perceived reduction in risk. Industry groups with whom we spoke indicated that their member companies face the challenge of effectively

allocating limited security resources. Facilities must also determine what constitutes a reasonable level of security against known or suspected threats. For example, officials noted that preparing facilities against extreme terrorist scenarios, such as jetliner attacks, would be prohibitively expensive.

Third, facilities face pressure from public interest groups to implement inherently safer practices (referred to in the industry as inherently safer technologies), such as lowering toxic chemical inventories and redesigning sites to reduce risks. Justice, in introducing its methodology to assess chemical facilities' vulnerabilities, also recognized that reducing the quantity of hazardous material may make facilities less attractive to terrorist attack and reduce the severity of an attack. While industry recognizes the contribution that inherently safer technologies can make to reducing the risk of a terrorist attack, industry officials noted that decisions about inherently safer technologies require thorough analysis and may shift, rather than reduce, risks. For example, reducing the amount of chemicals stored may shift the risk onto the transportation sector as reliance on rail or truck shipments increases. Finally, industry officials underscored that relocating chemical storage tanks and other site redesign strategies may be extremely costly and may have repercussions on other facility operations.

Fourth, industry officials voiced concern about government agencies' ability to protect sensitive information relating to facility vulnerabilities and security. They stated that companies may be hesitant to share information about site-specific vulnerabilities and security unless government agencies implement specific safeguards to protect this information. We have also reported that public-private information sharing practices are central to critical infrastructure protection. Specifically, practices such as taking steps to ensure that sensitive information is not inappropriately disseminated and developing standards and agreements on how shared information will be used and protected are critical to successful information sharing.[23]

Finally, industry officials stated that the industry faces a challenge in engaging all chemical facilities in voluntary security efforts. Industry officials noted that facilities that are not ACC members present a concern

[23]U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

because they may not be addressing security issues. Officials expressed concern that smaller chemical companies may not be taking as much action as larger companies to address vulnerabilities. Officials also mentioned ACC's efforts to engage other facilities that manufacture, distribute, transport, store, or dispose of chemicals through the Responsible Care program, noting that failure of all facilities to act may affect public perception of the efficacy of voluntary industry initiatives.

Although the industry has taken steps to address security concerns, the extent of security preparedness across the chemical industry is unknown. Currently, no federal agency has assessed the extent of security preparedness across the nation's chemical facilities. EPA officials stated that they do not know the extent that all facilities are addressing security issues. During its work developing a chemical facility vulnerability assessment methodology, Justice observed that some facilities may need to implement more effective security systems and develop alternative means to reduce the potential consequences of a successful attack.

Conclusions

Across the nation, thousands of industrial facilities manufacture, use, or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk of injury or death in the event of a chemical release. Yet, despite all efforts since the events of September 11, 2001, to protect the nation from terrorism, the extent of security preparedness at U.S. chemical facilities is unknown. While some other critical infrastructures are required to assess their security vulnerabilities, no federal requirements are in place to require chemical facilities to assess their vulnerabilities and take steps to reduce them. EPA believes the Clean Air Act could be interpreted to require security actions at chemical facilities, but the agency is currently taking a voluntary approach, leaving it to industry to make improvements the industry believes are warranted. However, no federal oversight or third-party verification ensures that voluntary industry assessments are adequate and that necessary corrective actions are taken. Furthermore, the sharing of information about facility vulnerabilities and security practices, without the risk of compromising sensitive information, among facilities and federal, state, and local government would provide each group with the ability to respond appropriately to any security threat. Our work demonstrates the need to move to a comprehensive national strategy that does more to assure the Congress and the public that chemical facilities have taken appropriate security measures. By swiftly implementing a comprehensive approach to reduce the risk of a terrorist-caused release, policymakers can better protect American communities.

Recommendations for Executive Action

In order to ensure that chemical facilities take action to review and address security vulnerabilities, we recommend that the Secretary of Homeland Security and the Administrator of EPA jointly develop, in consultation with the Office of Homeland Security, a comprehensive national chemical security strategy that is both practical and cost effective. This national strategy should

- identify high-risk facilities based on factors including the level of threat and collect information on industry security preparedness;
- specify the roles and responsibilities of each federal agency partnering with the chemical industry;
- develop appropriate information sharing mechanisms; and
- develop a legislative proposal, in consultation with industry and other appropriate groups, to require these chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action.

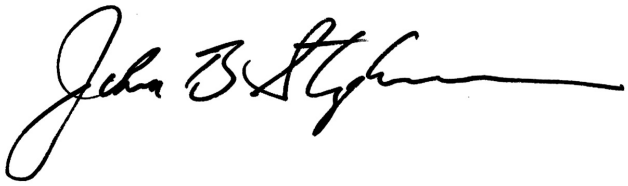
Agency Comments

We provided the Departments of Homeland Security and Justice, and EPA with a draft of this report for review and comment. These agencies generally agreed with the report's findings and conclusions. EPA also provided a number of technical comments and clarifications, which we incorporated in the report as appropriate. The Department of Homeland Security and EPA agreed that legislation requiring chemical facilities to assess and address vulnerabilities to terrorist attack should be enacted. Both agencies noted that the February 2003 President's National Strategy for the Physical Protection of Critical Infrastructures and Key Assets asks the Department of Homeland Security, in concert with the White House, EPA, and other key departments and agencies, to work with Congress to enact legislation to help protect the American public by requiring certain chemical facilities, particularly those that maintain large quantities of hazardous chemicals near population centers, to perform vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified. We revised our report to include the President's newly released strategy for protecting the chemical industry infrastructure. In responding to our draft, Justice commented that our report failed to state Justice's conclusion that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible. We revised our report to address Justice's comments and made other revisions as appropriate. The Department of Homeland Security and Justice provided written comments, which appear in appendixes I and II, respectively.

We performed our work from April 2002 through March 2003 in accordance with generally accepted government auditing standards.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time, we will send copies of this report to other interested parties and make copies available to others who request them. In addition, the report will be available at no charge at GAO's Web site at http:www.gao.gov.

If you or your staff have any questions about this report, please call me or Peg Reese, Assistant Director, at (202) 512-3841. Key contributors to this report are listed in appendix IV.



John B. Stephenson
Director, Natural Resources
and Environment

List of Congressional Requesters

The Honorable W.J. "Billy" Tauzin
Chairman
The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

The Honorable Frank Pallone, Jr.
House of Representatives

The Honorable John Shimkus
House of Representatives

Appendix I: Comments from the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

38095

U.S. Department of Homeland Security

February 24, 2003

John Stephenson
Director
Natural Resources & Environment
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Stephenson:

Thank you for the opportunity to review and comment on the GAO Report on Chemical Facility Security. This letter transmits our comments on the draft report.

The President, Secretary Ridge and the Department of Homeland Security are committed to protecting America's communities and families across the board, including the priority of reducing the vulnerability of America's chemical facilities to terrorist attacks. Secretary Ridge has publicly acknowledged the voluntary efforts that many private sector entities have undertaken to address this important issue. However, as also publicly stated by the Secretary, voluntary efforts alone will not be sufficient to assure an appropriate level of security across the chemical industry.

The Department's view is that every one of the approximately15,000 chemical facilities nationwide that contains significant quantities of highly hazardous chemicals should be required to take the steps that many industry leaders are undertaking at their facilities: performing comprehensive vulnerability assessments and then taking action to reduce those vulnerabilities.

See comment 1.

The President, in the recently released *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* has outlined the Administration's near-term road-ahead for addressing important security concerns associated with the chemical sector. As detailed in this document, the President has asked the Department of Homeland Security, in concert with the White House, the Environmental Protection Agency and other key departments and agencies, to work with Congress to enact legislation to help protect the American public by requiring certain chemical facilities, particularly those that maintain large quantities of hazardous chemicals in close proximity to population centers, to perform vulnerability assessments and take reasonable steps to reduce the vulnerabilities identified. The Department looks forward to working with Congress to advance this important homeland security initiative.

Sincerely,

Ken Hill
Executive Secretary

Washington, D. C. 20528

The following is GAO's comment on the Department of Homeland Security's letter dated February 24, 2003.

GAO Comment

1. We revised our report to include the President's newly released strategy for protecting critical infrastructures.

Appendix II: Comments from the Department of Justice

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Justice

Washington, D.C. 20530

FEB 28 2003

Mr. John Stephenson
Director, Natural Resources and Environment
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Stephenson:

Thank you for the opportunity to review the final draft of the General Accounting Office (GAO) report entitled "Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown, GAO-03-439." The draft was reviewed by representatives of the Department's Criminal Division, Federal Bureau of Investigation (FBI) and Office of Justice Programs. This letter constitutes the formal comments of the Department of Justice, and I request that it be included in the final report.

Under the Results and Brief section of your draft report, you mention that the federal government has not comprehensively assessed the chemical industry's vulnerabilities to terrorist attacks and imply that since this comprehensive assessment has not been completed, federal, state, and local entities lack comprehensive information on the vulnerabilities industry faces. Your report addresses preliminary steps taken by the Environmental Protection Agency (EPA) and the Department of Homeland Security (DHS), and the Department of Justice's (DOJ) interim report to Congress that described observations on security at 11 chemical manufacturing facilities to assist the industry in its preparedness efforts, but it fails to mention that the federal government is currently assessing the overall weapons of mass destruction (WMD) threat to the Homeland. This assessment is expected to be completed in April 2003.

See comment 1.

In 1995, Presidential Decision Direction-39 was signed which designated the FBI as lead federal agency for the operational response to terrorism. As such, the FBI is responsible for conducting WMD threat assessments and managing the operational response to WMD terrorism. The FBI's WMD Operations Unit and National Infrastructure Protection Center have been proactive in meeting with members of the chemical industry and other agency experts to share intelligence and facilitate liaison. As the lead federal agency, the FBI has taken steps to contact chemical manufacturers via WMD Coordinators in each of the 56 FBI field divisions. Chemical Outreach booklets have been provided to manufacturers to provide a brief overview of indicators and precursors that are known to be used as chemical weapons, as well as help them identify and report suspicious activities to the FBI. Further, the DOJ works closely with the chemical industry, most notably the American Chemistry Council (ACC), and information pertaining to the threats and vulnerabilities of industry is regularly addressed.

Mr. John Stephenson 2

The Department previously advised GAO that there was an inaccuracy in the prior draft report which stated that no credible evidence exists that a US chemical facility has been targeted by terrorists. This final draft report was revised to read: "At the time of our review, Justice officials told us that they had no credible evidence that any U.S. chemical facility has been the target of a person or group linked to terrorism. However, experts agree that chemical facilities may be attractive targets for terrorists intent on causing massive damage because many facilities house toxic chemicals that could become airborne and drift to surrounding areas if released. Alternatively, terrorists could steal chemicals, which could be used to create a weapon capable of causing harm. In fact, according to Justice, criminals attempted to release chemicals from facilities in the United States on at least two occasions during the late 1990s."

See comment 2.

The GAO's revised paragraph continues to be inaccurate, both in its portrayal of the Department's assessment of potential targeting by terrorists of chemical facilities and by suggesting that the Department does not have information on cases or intelligence relating to the targeting of such facilities. It suggests that the Department, as contrasted with unidentified experts, has never thought chemical facilities would be an attractive target for terrorists. In fact, the Department has been warning of the terrorist threat to such facilities for a number of years and our risk assessment in 2000, conducted at the direction of the President and pursuant to the Clean Air Act (CAA), concluded in no uncertain terms that chemical facilities present attractive targets for terrorists. On page 2 of the "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," the assessment states, "Based on our analysis of trends in international and domestic terrorism and upon the burgeoning interest in weapons of mass destruction (WMD) among criminals and terrorists, we have concluded that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible."

Further, your draft report refers to two incidents when "criminals" attempted to release chemicals from facilities. In one instance, criminals acting with non-terrorism motives attempted to release chemicals from a facility in the United States in the late 1990's. The other incident was a Sacramento, California terrorist-related incident. It is inaccurate to describe it as simply a "criminal" incident. The Sacramento incident was an instance where in 1998-99, domestic terrorists plotted to use a destructive device against a facility outside of Sacramento which housed millions of gallons of propane. This is credible evidence that chemical facilities presented an attractive target for terrorists. Since September 11th, the threat of potential attack against chemical facilities has only increased. In testimony on February 6, 2002, Director Tenet, Central Intelligence Agency, warned of the potential for an attack by al Qaeda on chemical facilities.

In the report section "An Attack Against Chemical Facilities Could Cause Economic Harm and Loss of Life" you discuss the security vulnerability findings at 11 chemical facilities assessed by the Department. Further, you discuss the security vulnerabilities at some facilities based on media accounts. The manner in which it is written implies that the Department's assessments could have been based on media reports. This is not correct and should not be implied.

Mr. John Stephenson 3

The discussion of EPA's potential reliance on either the risk management plan or general duty clause of the CAA to regulate chemical site security notes the drawbacks of relying on the CAA in such a manner and specifically notes a Department of Labor objection. This has also been a long-standing concern of the DOJ. The Department's position is that the CAA does not provide sufficient protection against dissemination of sensitive information, such as vulnerability assessments, that could be used by terrorists for targeting. We have voiced these concerns repeatedly in interagency meetings. Given the significance of this concern, GAO's current description of the drawbacks of relying on the CAA is substantially incomplete and, by omission, inaccurate in its description of the problems with the CAA approach.

See comment 3.

Your discussion regarding the Department's mandate to review and report on the vulnerability of chemical facilities to terrorist or criminal attack is also incomplete and misleading. As made clear in the National Institute of Justice's (NIJ) report, the Chemical Facility Vulnerability Assessment (CFVA) Project was undertaken by NIJ pursuant to language contained in the Conference Report (H.Rpt. 106-1005) which accompanied the DOJ Appropriations Act for FY 2001 (Pub.L. 106-553). Until the FY 2003 Omnibus Appropriations Act, signed by the President on February 20, 2003, no other direction on funding was made available by Congress to complete the report requirements of the Chemical Safety Information Site Security and Regulatory Relief Act (CSISSFRRA) (Pub.L. 106-40), despite the Department reprogramming requests for this task.

See comment 4.

According to the H. Rpt. 106-1005, NIJ was requested to develop, test, and validate a prototype national vulnerability assessment methodology for assessing the security of chemical facilities against terrorist and criminal attacks. Further, H. Rpt. 106-1005 stated that development of the assessment methodology was to be consistent with the requirements of CSISSFRRA. It requires the Attorney General to report to Congress on issues relating to the security and safety surrounding the manufacture and transport of chemicals. The CFVA Project report served as the basis for the Attorney General's interim report to Congress, which was required by CSISSFRRA.

The FY 2003 President's Budget requested $3 million to perform vulnerability assessments required under CSISSFRRA. H. Rpt. 108-010 accompanying P.L. 108-7 included the following direction concerning funding for the vulnerability assessments required under CSISSFRRA:

> *"The conferees expect that of the funding being transferred to the Department of Homeland Security from General Administration, that $3,000,000 shall be used for the chemical plant vulnerability assessments as authorized under Public Law 106-40."*

Finally, your description of the vulnerability assessment methodology developed by the NIJ does not include several important details. The methodology begins with a screening step to determine if a detailed vulnerability assessment is required. The methodology includes a complete assessment of the type, nature, physical characteristics, operational practices, and security systems at chemical facilities. Thus, the effectiveness of security systems are evaluated in light of the overall operation of the chemical facility.

See comment 5.

Mr. John Stephenson 4

Prior to risk analysis, the likelihood of various potential incidents is evaluated to allow facility managers to prioritize their response.

Again, we appreciate the GAO giving the Department an opportunity to comment in this process and thank the Congress for its support in our continuing efforts to improve our Homeland Security.

Sincerely,

Paul Corts
Assistant Attorney General
for Administration

The following are GAO's comments on the Department of Justice's letter dated February 28, 2003.

GAO Comments

1. As discussed in our report, we give credit to Justice for conducting threat assessments, working with industry to share intelligence and facilitate liaison, and contacting chemical facilities through field divisions to provide information and technical assistance.

2. We agree with Justice that chemical facilities could be an attractive target for terrorists. We have revised our report accordingly and have added that Justice believes that the risk of terrorists attempting in the foreseeable future to cause an industrial chemical release is both real and credible. We also included additional information on the 1998-99 domestic terrorist plot to use a destructive device at a facility that housed propane.

3. We revised our report accordingly to include Justice's longstanding concern that the Clean Air Act does not provide sufficient protection against dissemination of sensitive information, such as vulnerability assessments, that could be used by terrorists for targeting.

4. We disagree with Justice's position regarding its mandate to review and report on the vulnerability of chemical facilities to terrorist or criminal attack. Our October 2002 report (see footnote 3 on page 3) provides more detail on Justice's actions to fulfill the report requirements of the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA) and our views on this matter. We revised our report, however, to include discussion concerning the February 2003 Conference report on Justice's appropriation act for fiscal year 2003 that directed that $3 million of the funding transferred to the Department of Homeland Security be used for chemical plant vulnerability assessments authorized by CSISSFRRA.

5. We revised the report to include additional information on the vulnerability assessment methodology steps.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

John B. Stephenson (202) 512-3841
Peg Reese (202) 512-9695

Acknowledgments

In addition to those names above, Paige Gilbreath; Stan Kostayla; Linda Libician; Joanna McFarland; Carol Herrnstadt Shulman; Amy Webbink; and Leigh White made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER