

January 2006

# HOMELAND SECURITY

## DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed





Highlights of [GAO-06-150](#), a report to congressional requesters

## Why GAO Did This Study

Terrorist attacks on U.S. chemical facilities could damage public health and the economy. While the Environmental Protection Agency (EPA) formerly led federal efforts to ensure chemical facility security, the Department of Homeland Security (DHS) is now the lead federal agency coordinating efforts to protect these facilities from terrorist attacks.

GAO reviewed (1) DHS's actions to develop a strategy to protect the chemical industry, (2) DHS's actions to assist in the industry's security efforts and coordinate with EPA, (3) industry security initiatives and challenges, and (4) DHS's authorities and whether additional legislation is needed to ensure chemical plant security. GAO interviewed DHS, EPA, and industry officials, among others.

## What GAO Recommends

GAO recommends that (1) the Congress consider giving DHS the authority to require the chemical industry to address plant security, (2) DHS complete the chemical sector-specific plan in a timely manner, and (3) DHS work with EPA to study the security benefits to plants of using safer technologies. After reviewing a draft of this report, DHS agreed in substance with GAO's first two recommendations but expressed concerns about studying safer technologies. GAO continues to see merit in such a study. EPA had no comments on the draft report.

[www.gao.gov/cgi-bin/getrpt?GAO-06-150](http://www.gao.gov/cgi-bin/getrpt?GAO-06-150).

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

## HOMELAND SECURITY

# DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed

## What GAO Found

As part of a national framework for protecting the chemical sector, DHS is developing a Chemical Sector-Specific Plan. The plan is intended to, among other things, describe DHS's ongoing efforts and future plans to coordinate with federal, state, and local agencies and the private sector; identify chemical facilities to include in the sector, assess their vulnerabilities, and prioritize them; and develop programs to prevent, deter, mitigate, and recover from attacks on chemical facilities. DHS did not estimate when the plan will be completed.

To date, DHS has taken a number of actions aimed at protecting the chemical sector from terrorist attacks. DHS has identified 3,400 facilities that, if attacked, could pose the greatest hazard to human life and health and has initiated programs to assist the industry and local communities in protecting chemical facilities. For example, the Buffer Zone Protection Program assists facility owners and local law enforcement with improving the security of areas surrounding plants. DHS also coordinates with the Chemical Sector Coordinating Council, an industry-led group that acts as a liaison for the chemical sector, and with EPA and other federal agencies.

The chemical industry is voluntarily addressing plant security, but faces challenges in preparing against terrorism. Some industry associations require member companies to assess plants' vulnerabilities, develop and implement plans to mitigate vulnerabilities, and have a third party verify that security measures were implemented. Other associations have developed security guidelines and other tools to encourage their members to address security. While voluntary efforts are under way, industry officials said that they face challenges in preparing facilities against terrorism, including high costs and limited guidance on how much security is adequate.

Because existing laws provide DHS with only limited authority to address security at chemical facilities, it has relied primarily on the industry's voluntary security efforts. However, the extent to which companies are addressing security is unclear. Unlike EPA, for example, which requires drinking water facilities to improve their security, DHS does not have the authority to require chemical facilities to assess their vulnerabilities and implement security measures. Therefore, DHS cannot ensure that facilities are taking these actions. DHS has stated that its existing authorities do not permit it to effectively regulate the chemical industry, and that the Congress should enact federal requirements for chemical facilities. Many stakeholders agreed—as GAO concluded in 2003—that additional legislation placing federal security requirements on chemical facilities is needed. However, stakeholders had mixed views on the contents of any legislation, such as requirements that plants substitute safer chemicals and processes that potentially could reduce the risks present at these facilities.

---

# Contents

---

---

## Letter

Results in Brief	1
Background	4
DHS Is Developing a Plan for Protecting the Chemical Sector	8
DHS Has Taken Actions to Assess Facilities' Vulnerabilities and Interact with the Industry and Other Federal Agencies	17
The Chemical Industry Continues Voluntary Efforts to Address Security, but Faces Challenges in Safeguarding Facilities	20
DHS Needs Additional Authority to Ensure That Chemical Facilities Are Addressing Security Issues	35
Conclusions	43
Matters for Congressional Consideration	56
Recommendations for Executive Action	58
Agency Comments and Our Evaluation	58

---

## Appendixes

<b>Appendix I: Objectives, Scope, and Methodology</b>	62
<b>Appendix II: Summary of the Chemical Industry's Voluntary Security Initiatives</b>	65
<b>Appendix III: Comments from the Department of Homeland Security</b>	74
GAO Comments	79
<b>Appendix IV: GAO Contact and Staff Acknowledgments</b>	81

---

## Tables

Table 1: Number and Percentage of Processes That Involve More Than Threshold Amounts of Hazardous Chemicals under the RMP, by Industry Sector	10
Table 2: Overview of Key Chemical Security Legislative Proposals in the 109th Congress	14
Table 3: Examples of Federal Security Requirements for Other Critical Infrastructure Sectors	47

---

**Abbreviations**

ACC	American Chemistry Council
ASC	Adhesive and Sealant Council
CGA	Compressed Gas Association
CSISSFRRA	Chemical Safety Information, Site Security and Fuels Regulatory Relief Act
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FACA	Federal Advisory Committee Act
FDA	Food and Drug Administration
FOIA	Freedom of Information Act
IAIP	Information Analysis and Infrastructure Protection
IME	Institute of Makers of Explosives
ISAC	Information Sharing and Analysis Center
MTSA	Maritime Transportation Security Act
NACD	National Association of Chemical Distributors
NPCA	National Paint and Coatings Association
NPRA	National Petrochemical and Refiners Association
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
OMB	Office of Management and Budget
PCII	Protected Critical Infrastructure Information Program
RAMCAP	Risk Analysis Management for Critical Asset Protection
RMP	Risk Management Plan
SOCMA	Synthetic Organic Chemical Manufacturers Association
TFI	The Fertilizer Institute

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. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, D.C. 20548

---

January 27, 2006

The Honorable Susan M. Collins  
Chairman, Committee on Homeland Security  
and Governmental Affairs  
United States Senate

The Honorable James M. Inhofe  
Chairman, Committee on Environment  
and Public Works  
United States Senate

The Honorable Christopher Shays  
Chairman, Subcommittee on National Security,  
Emerging Threats, and International Relations  
Committee on Government Reform  
House of Representatives

Across the nation, approximately 15,000 facilities produce, use, or store more than threshold amounts of chemicals identified by the Environmental Protection Agency (EPA) as posing the greatest risk to human health and the environment if accidentally released into the air. These facilities include chemical manufacturers, storage and distribution facilities, fertilizer and pesticide facilities, pulp and paper manufacturers, water and wastewater treatment facilities, and refineries, among others. Since the events of September 11, 2001, government and other experts have recognized the potential threat that chemical facilities pose because many house toxic chemicals that could become airborne and drift to surrounding areas or be used to create a weapon capable of causing harm. In this regard, in 2003, the Department of Justice (Justice) reported that industrial chemical plants remain viable targets and warned that al Qaeda operatives may attempt to launch conventional attacks against U.S. chemical facilities to cause contamination, disruption, and terror. While these facilities potentially put large numbers of Americans at risk of injury or death in the event of a chemical release, the chemicals they produce, use, store, and distribute are critical to the nation's economy.

---

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and set forth its mission to, among other things, prevent terrorist attacks in the United States and reduce the vulnerability of the nation to terrorism.<sup>1</sup> The President's February 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets sets forth the federal government's roles, objectives, and responsibilities in protecting the nation's critical infrastructure, including the chemical industry. In addition, consistent with the Homeland Security Act, a December 2003 presidential directive instructed DHS to produce a comprehensive integrated plan outlining national goals, objectives, milestones, and key initiatives for protecting critical infrastructure and key resources. The directive also names DHS as the lead agency for the chemical sector, a change from earlier national strategies that named EPA as the lead.<sup>2</sup> Under an interim national plan released in February 2005, DHS is to identify and prioritize critical chemical facilities, evaluate the chemical sector's vulnerabilities and risks, develop and implement protective programs for high-priority chemical facilities, identify regulatory options for protective measures, and maintain a relationship with all stakeholders.

The federal government's role in protecting chemical facilities from terrorist attacks has been much debated since September 11, 2001. Public debate has centered on whether the federal government should impose security requirements on chemical facilities or continue to work with the chemical industry to voluntarily address security concerns. Legislative proposals that would grant DHS or EPA, or one of these agencies in consultation with the other, the authority to require chemical facilities to take security steps were introduced in every Congress from 2001 to 2005.

---

<sup>1</sup>Pub. L. No. 107-296, 116 Stat. 2145 (2002).

<sup>2</sup>Homeland Security Presidential Directive Number 7 (Washington, D.C.: Dec. 17, 2003).

---

In this context, you asked us to examine federal and industry efforts to address security concerns at chemical facilities. Specifically, this report discusses (1) DHS's actions to develop an overall strategy for protecting the chemical industry; (2) DHS's efforts to identify high-risk chemical facilities, assess their vulnerabilities, ensure that facilities are addressing security, and coordinate with EPA in these efforts; (3) chemical industry security initiatives and challenges; and (4) DHS's existing authorities and whether additional legislative authority is needed to ensure that chemical facilities take action to address vulnerabilities. In conducting our work, we interviewed officials from DHS's Information Analysis and Infrastructure Protection Directorate (IAIP), and EPA's Office of Emergency Management. We also reviewed pertinent federal legislation; EPA data; and DHS documents, including the Interim National Infrastructure Protection Plan, an early draft of the Chemical Sector-Specific Plan; and other available reports. We interviewed representatives of all 16 associations participating on the Chemical Sector Coordinating Council, a group of chemical sector associations that facilitate the sharing of industry views with DHS.<sup>3</sup> To obtain a broad range of industry views, we also spoke with at least one member company belonging to 13 of the key chemical industry associations.<sup>4</sup> These companies included large chemical manufacturers; small- and medium-sized chemical distributors; companies that manufacture, distribute, and sell agricultural and specialty chemicals; and plastics manufacturers, among others. We also interviewed other organizations with chemical industry expertise, including the American Society of Mechanical Engineers, the Center for Chemical Process Safety, Sandia National Laboratories, and the Working Group on Community Right-to-Know, among others. We conducted our work from December 2004 through December 2005 in accordance with generally accepted government auditing standards. A more detailed description of our objectives, scope, and methodology is contained in appendix I.

---

<sup>3</sup>As of November 2005, Chemical Sector Coordinating Council members included the Adhesive and Sealant Council; the American Chemistry Council; the American Forest & Paper Association; the Chemical Producers and Distributors Association; the Chlorine Chemistry Council; the Chlorine Institute; the Compressed Gas Association; CropLife America; the Fertilizer Institute; the Institute of Makers of Explosives; the International Institute of Ammonia Refrigeration; the National Association of Chemical Distributors; the National Paint and Coatings Association; the National Petrochemical and Refiners Association; the Society of the Plastics Industry, Inc.; and the Synthetic Organic Chemical Manufacturers Association.

<sup>4</sup>Three associations—the Adhesive and Sealant Council, the International Institute of Ammonia Refrigeration, and the National Paint and Coatings Association—were not able to identify a member company willing to speak with us.

---

---

## Results in Brief

As part of a national framework for reducing the overall vulnerability of the chemical sector in partnership with the industry and state and local authorities, DHS is developing a Chemical Sector-Specific Plan. Our review of a July 2004 draft of this plan—the most recent version available, according to DHS officials—and discussions with these officials on the contents of the final plan indicate that the plan will, among other things, describe

- the chemical industry, including providing background information and a detailed profile of the sector;
- the regulatory authority of key federal agencies relative to the chemical industry;
- DHS's coordination with federal, state, and local agencies, such as law enforcement and emergency management departments, and with the private sector on efforts that include sharing intelligence and security information;
- DHS's efforts to identify chemical facilities that should be included in the sector, assess their vulnerabilities, and prioritize these facilities on the basis of risk;
- DHS's development of protective programs in coordination with private and government entities to prevent, deter, mitigate, and recover from attacks on chemical facilities;
- how DHS will measure DHS and the industry's performance in addressing security issues, and research and develop new protective security measures; and
- challenges in improving security, including collecting information about facilities from a large number of owners, communicating with chemical facility owners who do not belong to industry associations, coordinating the roles of sector stakeholders, and working without federal regulatory authority.

DHS did not estimate when the plan will be completed.

In developing its plan for the chemical industry, DHS initiated several actions to identify the sector's critical assets, prioritize facilities, develop



---

and implement protective programs, exchange information with the private sector, and coordinate efforts with EPA and other federal agencies. DHS has determined the chemical sector's critical assets and identified about 3,400 high-priority facilities. In the future, however, the agency plans to use a new risk assessment methodology to compare and prioritize all critical infrastructure assets according to their level of threat, vulnerability to attack, and the consequences of an attack on the facility. To conduct this analysis, it will be necessary for chemical facility owners and operators to voluntarily assess and provide DHS with information on their vulnerabilities and potential consequences of an attack. DHS also has implemented a number of programs to assist the private sector and local communities in protecting chemical facilities. For example, DHS has conducted vulnerability assessments at 38 chemical facilities and shared suggestions for improvement with the facility owners and operators. In addition, DHS has worked with facility owners and local law enforcement to improve the security of areas surrounding a few high-risk chemical facilities in order to make launching an attack more difficult. DHS also shares threat information with the industry and coordinates sector activities with the Chemical Sector Coordinating Council, an industry-led working group that acts as a liaison for the chemical sector. Finally, DHS coordinates its chemical security efforts with EPA and other federal agencies through a government coordinating council.

The chemical industry, led by its industry associations, has undertaken voluntary efforts to address plant security, but faces challenges in preparing facilities against terrorism. As we reported in March 2005, some industry associations require member companies to assess their facilities' vulnerabilities and make security enhancements.<sup>5</sup> Three industry associations—the American Chemistry Council, the National Association of Chemical Distributors, and the Synthetic Organic Chemical Manufacturers Association—require as a condition of membership that companies conduct vulnerability assessments, develop and implement plans to mitigate vulnerabilities, and have a third party verify that the security enhancements were implemented. Other industry associations have encouraged their members to address security by developing security guidelines, best practices, and other tools. For example, a number of associations, including CropLife America, the Fertilizer Institute, and the

---

<sup>5</sup>GAO, *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges*, GAO-05-327 (Washington, D.C.: Mar. 28, 2005).

---

National Petrochemical and Refiners Association, have developed guidelines and vulnerability assessment methodologies tailored specifically to their member companies' unique security concerns. While efforts are under way to address security, industry officials told us that they face a number of challenges in preparing facilities against a terrorist attack. They reported that the cost of security improvements can be a burden, particularly for smaller companies that may lack the resources larger chemical companies have to devote to security. Industry officials stated that federal assistance via grants or tax incentives to offset security costs could help them enhance security at facilities. Industry officials also cited the need for guidance on what level of security is adequate, noting that determining the appropriate level of security for different facilities is difficult.

Existing laws provide DHS with only limited authority to address security concerns at U.S. chemical facilities. Because chemical facilities pose significant risks to millions of Americans, additional legislation is needed to give DHS the authority to require security improvements at these facilities. In this regard, DHS lacks the specific authority to require chemical facilities to assess their vulnerabilities and implement security measures. In addition, DHS currently lacks the authority to enter most chemical facilities without their permission for the purposes of assessing security or to enforce the implementation of any needed security improvements. Because, in contrast to some other critical infrastructure facilities—such as nuclear and drinking water facilities—chemical plants generally are not subject to federal security requirements, DHS has relied primarily on the voluntary participation of the private sector to address facility security. As a result, DHS cannot ensure that all high-risk facilities are assessing their vulnerability to terrorist attacks and taking corrective actions, where necessary. On this basis, we concluded in 2003 that additional legislation is needed to place federal security requirements on chemical facilities. Similarly, many of the stakeholders we contacted—including representatives from industry, research centers, and government—agreed on the need for additional legislation that would establish federal security requirements. These stakeholders had mixed views, however, on the specific contents of any legislation, such as requirements that facilities substitute safer chemicals and processes—referred to as “inherently safer technologies”—that could lessen the potential consequences of an attack by reducing the risks present at these facilities, but could be costly or infeasible for some plants. Finally, DHS also has concluded that its existing authorities do not permit it to effectively regulate the industry, and that the Congress should enact federal

---

requirements for chemical facilities. Given that the nation's chemical facilities pose significant risks and the extent of their security preparedness is largely unknown, legislation giving DHS the authority to require the chemical industry to address security at their plants could help to better protect these facilities against a potential terrorist attack.

We are recommending that the Congress consider providing DHS with the authority to require high-risk chemical facilities to assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action. We are also recommending that DHS complete the Chemical Sector-Specific Plan in a timely manner and work with EPA to study the advantages and disadvantages of substituting safer chemicals and processes at some chemical facilities. In commenting on a draft of this report, DHS agreed that the Congress should consider granting DHS the authority to require the chemical industry to address plant security and that completing and implementing the sector-specific plan is a priority. However, DHS disagreed with our recommendation that the department work with EPA to study the security benefits to chemical plants of using safer technologies. DHS believes that the use of safer technologies would not generally result in more secure chemical facilities and would tend to shift risks rather than eliminate them. DHS also stated that it is unclear what role EPA would play in a study of the benefits of using safer technologies or how DHS's interaction with EPA might be perceived among DHS's private sector partners.

---

---

## Background

Experts agree that chemical facilities present an attractive target for terrorists intent on causing massive damage. Terrorist attacks involving the theft or release of certain chemicals could significantly impact the health and safety of millions of Americans; disrupt local or regional economies; or impact other critical infrastructures that rely on chemicals, such as drinking water and wastewater treatment systems. The disaster in Bhopal, India, in 1984, when methyl isocyanate—a highly toxic chemical—leaked from a tank, reportedly killing about 3,800 people and injuring anywhere from 150,000 to 600,000 others, illustrates the potential threat to public health from a chemical release. As we reported in 2003, 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.<sup>6</sup> On the basis of analysis of trends in international and domestic terrorism and the burgeoning interest in weapons of mass destruction among criminals and terrorists, Justice warned of potential targeting of chemical facilities by terrorists even before the events of September 11, 2001. 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. According to news reports, terrorists also have targeted chemical facilities in Europe. Furthermore, on May 15, 2005, bombs were detonated in Spain by suspected Basque separatists at two chemical plants, a paint factory, and a metal works facility, leading to minor injuries from toxic fume inhalation.

No one has yet comprehensively assessed security at the nation's chemical facilities. In April 2005 testimony before the Senate Committee on Homeland Security and Governmental Affairs on chemical facility security, experts from the Council on Foreign Relations and the Brookings Institute underscored the threat that U.S. chemical facilities pose and expressed concern about the adequacy of security at these facilities. While federal and state governments and the chemical industry have taken steps to address security at chemical facilities, recent studies and media exposés have raised doubts about security at some plants. According to media accounts, every year from 2001 to 2005, reporters and environmental activists gained access to chemical tanks and computer centers that control manufacturing

---

<sup>6</sup>GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, GAO-03-439 (Washington, D.C.: Mar. 14, 2003).

---

processes at a number of facilities, including American Chemistry Council (ACC) member company facilities. In addition, a 2004 survey of employees at 189 chemical facilities conducted for the Paper, Allied-Industrial, Chemical, and Energy Workers International Union found that employees had doubts about the effectiveness of facilities' efforts to prevent a terrorist attack. Less than half of the respondents (44 percent) indicated that their companies' preventative actions, including security efforts, were effective in reducing facility vulnerabilities to terrorist attack. The U.S. Chemical Safety and Hazard Investigation Board also testified in April 2005 that gaps in safety and emergency response preparedness at chemical facilities leave Americans vulnerable. Furthermore, some environmental and advocacy groups believe reducing safety risks should be an integral part of facilities' efforts to reduce the potential consequences of a terrorist attack. These groups advocate reducing the inherent risks that toxic chemicals present by substituting safer chemicals or switching to inherently safer technologies.

---

## Universe of Chemical Facilities

EPA regulates about 15,000 facilities under the Clean Air Act because they produce, use, or store more than certain threshold amounts of specific chemicals that would pose the greatest risk to human health and the environment if they were accidentally released into the air. These facilities must take a number of steps, including preparing a risk management plan (RMP), to prevent and prepare for an accidental release and, therefore, are referred to as RMP facilities. These facilities fall within a variety of industries and produce, use, or store a host of products, including (1) basic chemicals used to manufacture other products, such as fertilizers, plastics, and synthetic fibers; (2) specialty chemicals used for a specific purpose, such as a functional ingredient or a processing aid in the manufacture of a range of products, including adhesives and solvents, coatings, industrial gases and cleaners, and water management chemicals; (3) life science chemicals consisting of pharmaceuticals and pesticides; and (4) consumer products, such as hair and skin products and cosmetics. Some of these facilities are part of critical infrastructure sectors other than the chemical sector. For example, about 2,000 of these facilities are community water systems that are part of the water infrastructure sector. In addition, other facilities that house hazardous chemicals that are listed under the RMP regulations are not subject to RMP requirements because the quantities stored or used are below threshold amounts. However, these facilities could also potentially be at risk of terrorist attacks. Table 1 outlines the number and percentage of processes in different industry sectors that involve more than threshold amounts of hazardous chemicals.

**Table 1: Number and Percentage of Processes That Involve More Than Threshold Amounts of Hazardous Chemicals under the RMP, by Industry Sector**

<b>Industry sector</b>	<b>Number of processes</b>	<b>Percentage of processes</b>
Agriculture and farming, farm supply, fertilizer production, and pesticides	5,767	29%
Water supply and wastewater treatment	3,456	17
Chemical manufacturing	3,758	19
Energy production, transmission, transport, and sale	3,045	15
Food and beverage manufacturing and storage (including refrigerated warehousing)	2,531	13
Chemical warehousing (not including refrigerated warehousing)	238	1
Other <sup>a</sup>	1,033	5
<b>Total<sup>b</sup></b>	<b>19,828</b>	<b>100%<sup>c</sup></b>

Source: EPA.

<sup>a</sup>“Other” represents a large variety of industry sectors, including pulp mills, iron and steel mills, cement manufacturing, and computer manufacturing.

<sup>b</sup>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., multiple processes containing more than a threshold amount of a covered hazardous chemical).

<sup>c</sup>Percentages do not total 100 percent due to rounding.

---

---

## The Federal Government's Roles and Responsibilities in Protecting the Chemical Sector

The Homeland Security Act established DHS and set forth its mission to, among other things, prevent terrorist attacks within the United States, reduce the nation's vulnerability to terrorism, and minimize the damage from and assist in the recovery from terrorist attacks that occur within the United States. The act also established DHS's IAIP and made it responsible for critical infrastructure protection and information analysis functions.<sup>7</sup> As part of its statutory responsibilities, IAIP must develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States. IAIP's other responsibilities include identifying threats, conducting comprehensive assessments of the vulnerabilities of key resources, conducting risk assessments to determine the risks posed by certain types of terrorist attacks, identifying priorities for protective measures, and recommending measures to protect critical infrastructure and key resources. The Secretary of the Department of Homeland Security has given IAIP responsibility for creating and managing private sector advisory councils composed of representatives of industries and associations designated by the Secretary to advise the Secretary on various matters, including private sector products, applications, and solutions, as they relate to homeland security challenges.<sup>8</sup>

This act and the December 2003 presidential directive established the framework under which IAIP carries out its responsibilities for coordinating the overall national critical infrastructure protection effort. The directive designates a lead federal agency for each critical infrastructure sector, such as agriculture, banking and finance, and chemical. DHS is now the lead, or sector-specific agency, for the chemical infrastructure, which is a change from national strategies issued in July 2002 and February 2003 that named EPA as the lead agency. IAIP is responsible for infrastructure protection activities for the chemical sector, including developing a plan for protecting the chemical sector by July 2004. Other IAIP chemical sector responsibilities include

- collaborating with relevant federal agencies, state and local governments, and the private sector;

---

<sup>7</sup>In November 2005, DHS reorganized the department. DHS divided the responsibilities of IAIP between DHS's Preparedness Directorate and a new Office of Intelligence and Analysis.

<sup>8</sup>The Homeland Security Act called upon the Secretary of DHS to appoint a special assistant to be responsible for these functions. See 6 U.S.C. § 112(f)(4).

- 
- conducting or facilitating vulnerability assessments of the chemical sector;
  - encouraging risk management strategies to protect against and mitigate the effects of attacks against chemical sector assets; and
  - collaborating with the appropriate private sector entities and continuing to encourage the development of information-sharing and analysis mechanisms and to support sector coordinating mechanisms.

In February 2005, DHS released an Interim National Infrastructure Protection Plan that also outlines the responsibilities of sector-specific agencies. As the lead agency for the chemical sector, the national plan calls for DHS to identify and prioritize critical chemical facilities, evaluate the chemical sector's vulnerabilities and risks, develop and implement protective programs for high-priority chemical facilities, identify regulatory options for protective measures, and maintain a relationship with all stakeholders.

Currently, federal requirements address security at some U.S. chemical facilities. A small number of chemical facilities must comply with the Maritime Transportation Security Act of 2002 (MTSA). MTSA and its implementing regulations require maritime facility owners and operators to conduct assessments of certain at-risk facilities to identify vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement the measures discussed in the security plans. MTSA and implementing regulations also require that the United States Coast Guard conduct inspections at these facilities and prohibit operation of facilities that do not have required security plans approved by the Secretary or that are not operating in compliance with these plans. According to July 27, 2005, testimony before the Senate Homeland Security and Governmental Affairs Committee, the Coast Guard has reviewed and approved facility security plans for 300 chemical facilities.

Some states and localities have also created security requirements at chemical facilities. For example, Maryland's Hazardous Material Security Act requires RMP facilities in the state to perform vulnerability assessments, develop and implement security measures, and report to the state Department of the Environment. Under New York's Anti-Terrorism Preparedness Act of 2004, the state Office of Homeland Security, subject to available appropriations, must require certain chemical facilities to conduct vulnerability assessments. Under the Domestic Security



---

Preparedness Task Force established by New Jersey law, New Jersey Department of Environmental Protection officials work with the state's chemical facilities to adopt security best practices. In addition, Baltimore, Maryland, requires chemical manufacturers to follow a set of safety and security regulations devised by its fire and police commissioners; noncompliance can result in penalties, such as the withholding or suspension of facility operating permits.

Separate from its responsibilities for enhancing the protection of the chemical sector from terrorist attacks, the federal government imposes safety and emergency response requirements on chemical facilities that may incidentally reduce the likelihood and consequences of terrorist attacks. For example, the Emergency Planning and Community Right to Know Act requires owners and operators of facilities that maintain specified quantities of certain extremely hazardous chemicals to annually submit information on their chemical inventory to state and local emergency response officials. This information is used to help prepare community response plans in the event of a chemical incident. Furthermore, under the Clean Air Act, EPA requires owners and operators of RMP facilities to prepare and implement a plan to detect and prevent or minimize accidental releases. In addition to evaluating "worst-case" accidental release scenarios, facility owners and operators must implement a program to prevent accidental releases that includes safety precautions and maintenance, and monitoring and training measures, and they must have an emergency response plan. The Department of Labor's Occupational Safety and Health Administration's process safety management standard also requires facilities to assess and address the hazards of their chemical processes. All of these requirements could potentially mitigate a terrorist attack by (1) providing an incentive to facilities to reduce or eliminate chemicals below regulated threshold levels, (2) requiring facilities to implement measures to improve the safety of areas that are vulnerable to a chemical release, and (3) facilitating emergency response planning that increases preparedness for a chemical release—whether intentional or unintentional.

---

## Legislative Proposals

Since 2001, the Congress has considered a number of legislative proposals that would give the federal government a greater role in ensuring the protection of the nation's chemical facilities. These legislative proposals would have granted DHS or EPA, or one of these agencies in consultation with the other, the authority to require chemical facilities to conduct vulnerability assessments and implement security measures to address

their vulnerabilities. In the 109th Congress, three bills have been introduced but have not yet been acted upon: H.R. 1562, H.R. 2237, and S. 2145. Table 2 provides an overview of the major provisions of these legislative proposals.

**Table 2: Overview of Key Chemical Security Legislative Proposals in the 109<sup>th</sup> Congress**

Major provisions	H.R. 1562	H.R. 2237	S. 2145
General requirements	High-priority facilities would be required to submit vulnerability assessments and security plans to DHS; other chemical sources would be required to self-certify completion of assessments and plans and provide DHS copies upon request.	High-priority facilities would be required to submit vulnerability assessments and to certify that they have prepared prevention, preparedness, and response plans to EPA.	Designated chemical sources would be required to submit vulnerability assessments, security plans, and emergency response plans to DHS. The assessment and security plan would be required to address security performance standards established by DHS for each risk-based tier. Chemical sources would be required to self-certify completion of assessments and plans.
Role of DHS and EPA	DHS, in consultation with EPA, would identify high-priority categories of facilities; DHS would receive and review assessments and plans.	EPA, in consultation with DHS and state and local agencies, would identify high-priority categories of facilities; EPA would receive assessments and certifications.	DHS would designate facilities as chemical sources and assign each chemical source to a risk-based tier. DHS would receive and review assessments, plans, and certifications. EPA would have no role.

(Continued From Previous Page)

Major provisions	H.R. 1562	H.R. 2237	S. 2145
Compliance enforcement	DHS would, when and where it deems appropriate, conduct or require the conduct of vulnerability assessments and other activities to ensure and evaluate compliance; DHS could disapprove a vulnerability assessment or site security plan; following written notification and consultation with the owner or operator, DHS could issue a compliance order.	Not later than 3 years after the deadline for submission of vulnerability assessments and response plans, EPA, in consultation with DHS, would review and certify compliance of each assessment and plan; following consultation with DHS, and 30 days after providing notification to the facility and providing advice and technical assistance to bring the assessment or plan into compliance and address threats, EPA could issue a compliance order.	DHS would review and approve or disapprove all vulnerability assessments, security plans, and emergency response plans for facilities in higher risk tiers within 1 year, and within 5 years for all other facilities. DHS would be required to disapprove of any vulnerability assessment, site security plan, or emergency response plan not in compliance with the vulnerability assessment, site security plan, and emergency response plan requirements. For higher risk facilities, if DHS disapproves the assessment or plans, the Secretary could issue an order to a chemical source to cease operation. For other facilities, the Secretary could issue an order to a chemical source to cease operation, but only after a process of written notification, consultation, and time for compliance.
Penalties for noncompliance	Would provide for court awarded civil penalties up to \$50,000 per day for failure to comply with an order, site security plan, or other recognized procedures, protocols, or standards, and administrative penalties up to \$250,000 for failure to comply with an order.	Would provide for court awarded civil penalties up to \$25,000 per day, criminal penalties, and administrative penalties (if the total civil penalties do not exceed \$125,000) for failure to comply with an order.	Would provide for court awarded civil penalties up to \$50,000 per day, and administrative penalties of not more than \$25,000 per day (not to exceed \$1 million per year) for failure to comply with a DHS order or directive issued under the act. Also calls for criminal penalties of up to \$50,000 in fines per day, imprisonment for not more than 2 years, or both for knowingly violating an order or failing to comply with a site security plan.
Inherently safer technologies requirements	None.	Response plans would be required to include a description of safer design and maintenance options considered and reasons those options were not implemented; EPA would be required to establish a clearinghouse for information on inherently safer technologies and would be authorized to provide grants to assist chemical facilities demonstrating financial hardship in implementing inherently safer technologies.	None.

(Continued From Previous Page)

Major provisions	H.R. 1562	H.R. 2237	S. 2145
Information protections	Would exempt information obtained from disclosure under the Freedom of Information Act (FOIA) or otherwise, or from disclosure under state or local laws; information would also not be subject to discovery or admitted into evidence in any federal or state civil judicial or administrative procedure other than in civil compliance action brought by DHS. Calls for DHS, in consultation with others, to establish confidentiality protocols.	Would exempt information obtained from disclosure under FOIA; calls for EPA, in consultation with DHS, to establish information protection protocols.	Would exempt information obtained from disclosure under FOIA, or from disclosure under state or local laws. Certifications submitted by the chemical sources, orders for failure to comply, and certificates of compliance and other orders would generally be made available to the public. Calls for DHS, in consultation with the Director of the Office of Management and Budget and appropriate federal law enforcement officials, to create confidentiality protocols for the maintenance and use of records; would establish penalties for the unlawful disclosure of protected information.
Equivalence of industry codes	Upon petition, DHS would be required to endorse other industry, state, or federal protocols or standards that the Secretary of DHS determines to be substantially equivalent.	None.	Would allow the Secretary to determine that vulnerability assessments, security plans, and emergency response plans prepared under alternative security programs meet the act's requirements and to permit submissions or modifications to the assessments or plans.
Other	Would grant DHS right of entry; would exempt facilities that are subject to MTSA (port facilities) or the Bioterrorism Act (community water systems). Except with respect to protection of information, would not affect requirements imposed under state law.	Would grant EPA right of entry; would authorize EPA to provide grants for training of first responders and employees at chemical facilities; would not affect requirements imposed under state law.	Would grant DHS right of entry; would exempt facilities that are subject to MTSA from certain area security requirements but these facilities would otherwise comply with the act's requirements. Would preserve the right of states to adopt chemical security requirements that are more stringent than the federal standard, as long as the state standard does not conflict with the federal standard.

Source: GAO analysis of proposed legislation.

Also in the 109<sup>th</sup> Congress, the conference committee for H.R. 2360, making appropriations for DHS for fiscal year 2006, directed DHS to

- submit a report to the Senate and House Committees on Appropriations by February 10, 2006, describing (1) the resources needed to implement mandatory security requirements for the chemical sector and to create a system for auditing and ensuring compliance with the security standards and (2) the security requirements and any reasons why the

---

requirements should differ from those already in place for chemical facilities that operate in a port zone;

- complete vulnerability assessments of the highest risk U.S. chemical facilities by December 2006, giving preference to facilities that, if attacked, pose the greatest threat to human life and the economy; and
- complete a national security strategy for the chemical sector by February 10, 2006.<sup>9</sup>

---

## DHS Is Developing a Plan for Protecting the Chemical Sector

As part of an overall National Infrastructure Protection Plan (NIPP), DHS is developing a plan for protecting the chemical sector that will establish a framework for reducing the overall vulnerability of the sector in partnership with the industry and state and local authorities. The NIPP will outline how DHS and relevant stakeholders will develop and implement the national effort to protect infrastructures across all sectors. In February 2005, DHS released an interim NIPP that provides a strategy for critical infrastructure protection and a means for discussion with critical stakeholders. The NIPP states that each sector-specific agency is responsible for developing, implementing, and maintaining a sector-specific plan for their sector. Each plan is supposed to outline strategies for (1) collaborating with all relevant federal departments and agencies, state and local governments, and the private sector; (2) identifying assets; (3) conducting or facilitating vulnerability assessments; and (4) encouraging risk management strategies to protect against and mitigate the effects of an attack. The Chemical Sector-Specific Plan will be an appendix to the NIPP. While DHS did not provide an estimated completion date for either the Chemical Sector-Specific Plan or the NIPP, DHS stated that the plan and the plans for the other critical infrastructure and key resource sectors will be completed within 6 months of approval of the NIPP.

As the agency with lead responsibility for the chemical sector, DHS is responsible for developing the chemical sector-specific plan. DHS completed a draft of the plan in July 2004. Since that time, DHS has worked to revise the plan to accommodate changes to DHS's risk management strategy, comments from stakeholders' review of the NIPP, and consultation with chemical sector stakeholders. While DHS officials told us

---

<sup>9</sup>H.R. Conf. Rep. No. 109-24 (2005).

---

that the structure of the final plan will differ from the July 2004 version, they said that the basic principles and content described in that draft will still be included in the final plan.

On the basis of our review of the draft plan and discussions with DHS officials, the final plan will

- present background information on the sector, including a description of (1) the types of assets that are considered part of the chemical sector; (2) the regulatory authority of key federal agencies relative to the chemical industry and the key stakeholders in the sector; (3) the roles and responsibilities of each stakeholder; and (4) DHS's coordination with federal, state, and local agencies, such as law enforcement and emergency management departments, and with the private sector on efforts that include sharing intelligence and security information;
- describe the process DHS will use to develop a comprehensive inventory of assets in the chemical sector, including plans for working with the private sector to develop this inventory, since the critical infrastructure in the chemical sector is predominantly privately owned and operated;
- describe DHS's efforts to identify and assess the vulnerabilities of chemical facilities and how DHS plans to prioritize these efforts on the basis of the vulnerability assessments;
- outline the protective programs that will be created to prevent, deter, mitigate, and recover from attacks on chemical facilities, and describe how DHS will work with private sector and government entities to implement these programs;

- 
- explain the performance metrics DHS will use to measure the effectiveness of DHS and industry security efforts and ensure that DHS meets its overall critical infrastructure goals, including (1) identifying and assessing the vulnerability of the nation's critical infrastructure and key resources; (2) ensuring the protection of the nation's critical infrastructure and key resources from terrorist attack; (3) establishing a collaborative environment across all levels of government and with the private sector to better protect the nation's critical infrastructure and key resources; and (4) coordinating and integrating, as appropriate, with other federal emergency management and preparedness activities, including the National Response Plan;<sup>10</sup>
  - document DHS's plans to work with stakeholders to review current federal research and development initiatives for prioritization and to identify gaps between the chemical sector's requirements and current projects in order to identify research and development needs; and
  - outline challenges the department faces in coordinating the efforts of the chemical sector, such as collecting information about facilities from a large number of owners; communicating with chemical facility owners who do not belong to industry associations; coordinating the roles of sector stakeholders; and working without federal regulatory authority.

Furthermore, in September 2005, the conference committee, in the conference report for the Department of Homeland Security Appropriations Act, 2006, directed DHS to complete a national security strategy for the chemical sector by February 10, 2006.<sup>11</sup> According to DHS, the department is preparing a high-level strategic document—the National Strategy for Securing the Chemical Sector—that is separate but complementary to the Chemical Sector-Specific Plan.

---

<sup>10</sup>DHS plans to use a metrics-based system of performance evaluation that will conform to the Government Performance and Results Act of 1993. DHS will have core metrics, which will be common across all sectors, and specific metrics for the chemical sector.

<sup>11</sup>H.R. Conf. Rep. No. 109-241 (2005).

---

Our March 2003 report on chemical security recommended that DHS develop a comprehensive national chemical security strategy that is both practical and cost-effective.<sup>12</sup> We recommended that the strategy identify high-risk facilities, collect information on industry security preparedness, specify the roles and responsibilities of each federal agency partnering with the chemical industry, and develop appropriate information-sharing mechanisms. If the final Chemical Sector-Specific Plan includes the elements DHS has described, it should meet the criteria set out in this recommendation.

---

## DHS Has Taken Actions to Assess Facilities' Vulnerabilities and Interact with the Industry and Other Federal Agencies

DHS has taken initial action to identify the chemical sector's critical assets, prioritize facilities, develop and implement protective programs, exchange information with the private sector, and coordinate efforts with EPA and other federal agencies. In this regard, DHS has identified about 3,400 chemical facilities as posing the greatest hazard to human life and health, and it is developing a new risk assessment methodology to compare and prioritize all critical infrastructure assets according to their level of threat, their vulnerability to attack, and the consequences of an attack on the facility. Furthermore, DHS has implemented a number of programs to assist the private sector and local communities in protecting chemical facilities, conducted site vulnerability assessments at 38 facilities, and installed cameras at some high-consequence facilities. DHS is also distributing threat information to the industry and coordinating sector activities with the Chemical Sector Coordinating Council, an industry-led working group that acts as a liaison for the chemical sector. Finally, DHS is coordinating with EPA and other federal agencies through a government coordinating council.

---

## DHS Is Conducting Efforts to Identify and Prioritize Facilities

As the chemical sector-specific agency, one of DHS's key responsibilities under the interim NIPP is to identify the assets of the chemical sector and prioritize them according to risk. DHS's ongoing efforts in this regard, once completed, should produce a methodology for identifying critical assets in the chemical sector and comparing assets across sectors.

## DHS Is Identifying High-Priority Sites

DHS has identified approximately 3,400 chemical facilities that it believes pose the greatest hazard to human life and health in the event of a terrorist

---

<sup>12</sup>GAO-03-439.



---

attack. To develop an inventory of the chemical sector's critical assets, DHS first had to define what the sector includes. According to DHS officials, in general, they consider the chemical sector to include facilities that manufacture, distribute, and store chemicals, but not retail facilities. The chemical sector also includes facilities that overlap with other critical infrastructure sectors. For example, refineries, while considered part of the energy sector, use large amounts of chemicals and are often colocated with chemical manufacturing facilities. In addition, water purification and sanitation facilities are part of the water sector, but they store large amounts of chemicals on-site. Similarly, agricultural facilities house toxic chemicals, such as fertilizers and pesticides.

While the chemical sector includes a large number of facilities, DHS is focusing its efforts for the sector by identifying high-priority facilities. As a starting point, DHS has adapted EPA's RMP database of facilities with more than threshold amounts of certain chemicals to develop an interim inventory of chemical facilities of concern in the event of a terrorist attack. DHS officials told us that, to prioritize facilities, they reduced the list of RMP facilities in the database by eliminating entries that were redundant and 3,000 facilities that were no longer in business or were no longer RMP facilities (e.g., they had reduced the volume of chemicals on-site below the RMP threshold).<sup>13</sup> Furthermore, DHS determined that 8,000 of the remaining sites were the responsibility of another critical infrastructure sector. For example, DHS removed water treatment and distribution facilities because they fall under the water critical infrastructure sector, which is the responsibility of EPA. In addition, DHS removed agricultural facilities, such as fertilizer and pesticide distributors. DHS's analysis resulted in approximately 4,000 facilities. According to DHS officials, DHS then conducted a consequence analysis of these remaining facilities to identify those that, if attacked, would endanger the largest number of lives. According to DHS, the analysis included the following:

- Reviewing the amount and toxicity of RMP materials stored at sites. For example, DHS eliminated some facilities with flammable chemicals

---

<sup>13</sup>EPA has expressed concern about DHS's analysis of the RMP database. According to EPA officials, the results of DHS's analysis appear to indicate that the data may have been manipulated incorrectly. For example, EPA does not agree that the database contains 3,000 facilities that are no longer in business or no longer RMP facilities. EPA officials offered to assist DHS with interpretation of the RMP database. In commenting on our report, DHS stated that the department is open to working with EPA to clarify DHS's methodology for interpreting the RMP database as it relates to risk.

---

because they would not create catastrophic effects when released. DHS focused on toxic chemicals that pose inhalation hazards and very high-order flammables and explosives.

- Reviewing the population density in the vicinity of facilities with large amounts of toxic chemicals. DHS modeled potential toxic plumes from facilities and revised the population estimates of the RMP worst-case scenarios to develop what they believe is a more realistic estimate of the population that a terrorist attack would harm.<sup>14</sup>
- Evaluating possible impacts of an intentional attack, instead of using the accidental release model used in the RMP program. For example, DHS evaluated the daytime versus the nighttime population surrounding facilities and the possible impact resulting from the release of the entire volume of chemicals at a facility during an attack. By contrast, the RMP analysis considers the impacts of the release of the chemical volume in the single largest container.
- Consulting with industry experts to identify facilities that, if attacked, could cause serious economic harm or the shortage of critical materials.

On the basis of this analysis, DHS identified approximately 3,400 chemical facilities where a worst-case scenario release potentially could affect over 1,000 people. According to DHS, 272 of these facilities could potentially affect more than 50,000 people. These 272 facilities include chemical manufacturing plants as well as some refineries located with petrochemical

---

<sup>14</sup>According to EPA officials, RMP worst-case scenario population estimates are not intended to represent the number of people that could be harmed by a toxic worst-case accident. EPA regulations require facilities to estimate the distance that a toxic gas cloud would travel before its concentration is diluted below a specified level and to report the entire population within that distance of the facility. EPA officials stated that in an actual release event, even one where worst-case conditions existed, the toxic chemical plume would generally impact a fraction of the reported population, since a toxic plume would only cover areas downwind of the facility. However, since it is impossible to predict the exact wind conditions that will be present during an accidental release, EPA regulations require facilities to report the entire population within a full 360-degree circle surrounding the facility, even though this population number will almost always significantly overestimate the number of people that could be harmed by the scenario. EPA officials refer to the population within the 360-degree circle around the facility as the “vulnerable zone” population. DHS determined that the maximum width of a toxic chemical plume is 60 degrees, not the full 360-degree circle surrounding a facility. Thus, DHS adjusted the RMP worst-case scenarios estimates to develop what they believe is a more realistic estimate of the potential impact of a worst-case, terrorist-caused chemical release.

---

facilities, wastewater treatment facilities, and other types of chemical facilities. In commenting on our report, DHS noted that it did not intend wastewater treatment facilities to be incorporated in the list of top facilities.

### DHS Is Piloting a Risk Analysis Tool to Prioritize Facilities

DHS is developing a new process known as Risk Analysis Management for Critical Asset Protection (RAMCAP) that will allow the department to apply a risk management approach to prioritize assets in all critical infrastructure sectors. According to DHS, RAMCAP will provide a common methodology, terminology, and framework for homeland security risk analysis and decision making that is intended to allow consistent risk management across all sectors. According to DHS, RAMCAP will improve DHS's ability to collect information on critical infrastructure assets, compare risks across assets, and increase owners' and operators' awareness of the vulnerabilities and consequences at their sites.

DHS contracted with the American Society of Mechanical Engineers to assist it in creating the RAMCAP methodology. In 2004, the society presented the methodology to academic and industry officials and incorporated their comments. The feedback from many industry officials conveyed that the methodology was complex, and that industry officials completing the methodology would need assessment tools with terminology specific to their sector. As a result, the society hired subcontractors with industry expertise to develop sector-specific vulnerability assessment methodologies for five sectors: (1) chemical, (2) nuclear power, (3) nuclear fuel storage, (4) petroleum refining, and (5) liquefied natural gas storage/terminals. According to a society official, the subcontractor developing the chemical sector methodology studied and incorporated elements from existing methodologies, such as those developed by Sandia National Laboratories and the American Institute for Chemical Engineers' Center for Chemical Process Safety. The RAMCAP chemical sector methodology differs from these methodologies in that it uses terminology and processes that will be consistent with other sector methodologies and will allow comparisons to be made from the results of facility assessments across sectors. To assist in the development of the chemical sector tools, the subcontractor created a committee composed of representatives from chemical companies, such as Dow, DuPont, and Air Products; trade associations; national laboratories; and other entities with expertise, such as the Center for Chemical Process Safety.

In the first step in the RAMCAP process, chemical facility owners/operators will voluntarily complete a screening tool (top screen)

---

through a secure Web site. The top screen helps identify the consequences of an attack at a facility, including the human, economic, and psychological impacts. It would also identify such things as whether a facility produces a product that is essential to the military or pharmaceutical industry, or that is critical to the delivery of water or energy. On the basis of the results of the screening tool, DHS will identify facilities of highest concern and ask them to voluntarily complete a security vulnerability assessment, the second step in the RAMCAP process. Facility owners/operators will be able to use the results of previous vulnerability assessments they may have conducted to assist them in completing the RAMCAP process. The security vulnerability assessment will include the following steps:

- assessment of facility characteristics, such as potential target areas and facility attractiveness to attack;
- threat characterization of specific scenarios of concern—these “benchmark threats” of concern to the government will allow cross-sector comparison;
- consequence analysis of the impacts that could be produced by an attack; and
- vulnerability assessment of a facility’s existing security measures in place, including mitigation, detection, and response capability.

According to DHS officials, DHS will work with industry associations to distribute the RAMCAP screening tool to the highest consequence chemical facilities. DHS officials expect that between 5 and 10 percent of those chemical facility owners/operators will be asked to complete the self-vulnerability assessment.

DHS has tested both the screening tool and the vulnerability assessment, and several private sector companies have also volunteered to pilot test the vulnerability assessment. In 2005, New York’s Office of Homeland Security, working with DHS, requested all chemical facilities in the state to complete the RAMCAP screening tool. According to industry officials, however, the companies that pretested the vulnerability assessment found the exercise valuable but difficult to complete. They said that DHS officials assisted their companies in completing the assessment and expressed concern that some owners/operators may have difficulty completing the assessment without DHS’s help. Some chemical company officials who had not participated in the pilot told us that they would be reluctant to complete

---

the RAMCAP assessment, citing concerns about the work involved, the need for DHS to collect the information, and the ability of DHS to safeguard information on the facilities' security vulnerabilities. In addition, DHS recognizes that it will have difficulty in collecting information about chemical facilities and verifying these data due to the large number of facilities in the sector. While DHS plans to work with industry associations to encourage owners/operators to share information, private sector participation will be voluntary, and some companies do not belong to industry associations and, therefore, may not be easily contacted. According to DHS's draft Chemical Sector-Specific Plan, DHS does not have the resources to verify asset data for all chemical facilities and will have to rely in large part on the accuracy of information submitted by the owners/operators and federal, state, and local agencies. However, DHS plans to verify submitted information relating to high-consequence facilities.

---

### DHS Has a Number of Programs to Assist the Private Sector in Reducing Vulnerabilities

DHS has implemented a number of programs designed to assist the department in assessing chemical industry vulnerabilities, develop best practices, and assist the private sector and law enforcement in improving the security of high-risk chemical facilities. These programs will help DHS gather needed information on facilities and the level of security preparedness of the industry.

*Buffer Zone Protection Program:* Through this program, DHS works with local law enforcement officials and facility owners to improve the security of the area surrounding the facility or "outside of the fence." Improving the security of this buffer zone makes it more difficult for a terrorist to conduct surveillance or launch an attack. In general, a DHS team will visit a chemical plant and consider the facility's vulnerabilities and the community's capability to prevent and respond to an attack. Then, DHS brings together the appropriate local emergency response officials and provides training on how to assess buffer zone security and identify specific measures to reduce or eliminate vulnerabilities. Local officials conduct an assessment and summarize their work and the protective measures needed in a Buffer Zone Protection Plan. DHS reviews the plan and provides funding assistance to the community for some of the protective measures. According to DHS officials, the process helps facilitate relationships between owners/operators and the various response and law enforcement entities in the community. Several company officials we contacted who had participated in buffer zone assessments agreed with DHS's assessment of the process. For example, one company told us that

---

the process helped them develop a relationship with the local police, who are not always involved in emergency response planning at facilities. After the buffer zone assessment, the local police now patrols the company's fence on every shift.

Prior to March 2005, the Buffer Zone Protection Program was a loan program. DHS purchased equipment directly for loan to the states for a 1-year period prior to formal transfer of ownership. DHS received buffer zone plans for 10 chemical facilities and loaned over \$260,000 in equipment to these jurisdictions. DHS also has conducted 63 technical assistance visits to assist chemical facility owners/operators and local law enforcement in assessing their buffer zone security.

In March 2005, DHS announced a targeted grant program for states to purchase equipment that will enhance security measures around facilities.<sup>15</sup> DHS identified 259 chemical manufacturing plants and storage and stockpile supply areas that are eligible under program guidelines for \$12.95 million from the Buffer Zone Protection Plan grant program. According to DHS officials, these are sites with 50,000 people living in close enough proximity that, if attacked, some portion of this population would be at risk of death or serious injury.<sup>16</sup> States may apply for these grants on the behalf of local jurisdictions that plan to implement protective measures.<sup>17</sup> The local jurisdictions must conduct a buffer zone assessment and prepare a plan requesting funds for equipment on an approved list. Before the state can allocate funds, the guidelines state that DHS must approve the buffer zone plan and spending plan. States have until April 30, 2006, to apply for these funds.

*Site assistance visits:* To assess and identify vulnerabilities at chemical facilities, DHS deploys teams of experts from both government and industry to facilities to conduct a site assistance visit. The teams

---

<sup>15</sup>The Department of Homeland Security Appropriations Act, 2005, made appropriations for DHS grant programs. DHS allocated \$92 million for buffer zone protection grants for all sectors, including the chemical sector.

<sup>16</sup>According to DHS's Buffer Zone Grant Guidance, these are sites that, if attacked, could cause death or serious injury to 50,000 or more people.

<sup>17</sup>The governor of each state has designated a state administrative agency that is responsible for preparing and submitting all grant application materials on behalf of the state. The administrative agency is the grantee—that is, it administers the funds for the state and allocates funds to responsible jurisdictions.

---

conducting the visits have subject matter expertise in various areas, including physical security measures, system interdependencies, and terrorist attack planning. The teams have a field template to guide their efforts, and a typical visit lasts 1 to 2 days. Officials at participating facilities receive assistance in addressing security issues at their sites and obtain current threat information. At the conclusion of the visit, DHS suggests mitigation measures for the company to consider. As a result of these visits, DHS learns valuable information about chemical facility vulnerabilities and obtains information to assist in developing reports and identifying training for industry.

As of June 15, 2005, DHS had conducted 38 site assistance visits at chemical facilities. These visits included trips to water/wastewater treatment facilities that store and use chemicals, major refineries, and chemical manufacturing facilities. DHS selected facilities to visit on the basis of a variety of factors, including whether the facility (1) would have significant economic or public health effects if attacked, (2) is near a special event of national significance, or (3) is in the vicinity where another site assistance visit is planned and whether the visit was requested by the owner/operator. DHS plans to conduct additional site assistance visits to chemical facilities in fiscal year 2006 on the basis of need.

*Maritime Transportation Security Act:* The Coast Guard, now under DHS, is responsible for the MTSA program at facilities located along waterways, including 238 chemical sites. Program regulations established a process and deadlines for maritime facilities to follow in assessing their security risks and preparing related plans to include actions to mitigate any identified vulnerabilities. The Coast Guard has approved plans for all of these facilities and completed on-site compliance inspections. The Coast Guard has stated that it will continue to visit annually these and all facilities subject to MTSA to ensure compliance. The Coast Guard has awarded Port Security Grants to a number of chemical facilities to provide assistance for physical security enhancements.<sup>18</sup>

*Other protective measure programs:* DHS will place 68 protective security advisors in metropolitan areas across the country. The advisors have experience related to vulnerability reduction and physical security and many have law enforcement or military backgrounds. The advisors serve as

---

<sup>18</sup>The Coast Guard provided 287 grants, including some to chemical facilities, totaling over \$100 million.

---

a liaison between federal efforts and those by the state, local, and private sector. The advisors have responsibility for assisting in identifying high-priority facilities, providing the local community with information on threats and best practices, and coordinating training and facility visits.

In addition, DHS has installed cameras for security monitoring at 10 high-consequence chemical facilities. These are facilities that could have a significant effect on public health or the national or regional economy if attacked. The cameras provide local law enforcement authorities with the ability to conduct remote surveillance of the areas surrounding the facility during elevated threat levels. State homeland security offices and DHS also have access and may monitor the facilities. Prior to the installation of cameras, Buffer Zone Protection Plans were completed at the sites that determined the need for additional surveillance. According to DHS officials, they are considering equipping additional sites with Webcams.

DHS also is planning a series of Comprehensive Reviews in areas with a large number of chemical facilities, focusing on facilities' security as well as emergency response capabilities in the local area. A team of federal officials from multiple agencies will plan and conduct the work in coordination with state and local officials.<sup>19</sup> The goal of these reviews is to assess the current security and response capabilities of individual facilities, local law enforcement, and emergency response organizations. The results of the review should help reduce disconnects between emergency response, law enforcement, and facilities and identify training, processes, and resources needed for the community. For these reviews, DHS will rely heavily on cooperation with facility owners/operators. DHS plans to conduct one visit to a cluster of facilities and then determine if it needs to improve the processes. DHS hopes to complete six visits to clusters of facilities during 2006.

---

<sup>19</sup>DHS stakeholders include the Office of Infrastructure Protection, Office for Domestic Preparedness, Federal Emergency Management Agency, United States Coast Guard, and Transportation Security Administration. Other federal stakeholders include the Environmental Protection Agency and the Federal Bureau of Investigation.



---

---

## DHS Shares Information with the Industry by Various Means

DHS is responsible for collaborating with the private sector in protecting critical infrastructure.<sup>20</sup> DHS's two main vehicles for coordinating and sharing information on threats, vulnerabilities, and best practices are the chemical sector Information Sharing and Analysis Center (ISAC) and an industry-led Chemical Sector Coordinating Council. DHS also is creating a new secure computer system to share information, provide best practice reports, and conduct training and drills.

In 2002, the federal government and ACC created the chemical sector ISAC to collect and share threat information for the chemical industry.<sup>21</sup> Through ISAC, DHS provides the private sector with threat information by means of daily electronic mail and a secure Web site. While ISAC was initially designed to allow companies to report unexplained or suspicious incidents involving chemical facilities, the system can no longer provide this function because of technical constraints. To operate the center, ACC uses its existing 24-hour communication network for sharing information about chemical emergencies. Any company engaged in the production, storage, transportation, sale, or delivery of chemicals may participate in ISAC's activities. ISAC has almost 600 participants representing more than 430 chemical companies that receive daily intelligence reports as well as episodic alerts and warnings. Some industry officials have complained about the lack of specific threat information they receive from DHS, and, in recent testimony, ACC called for more frequent and more detailed threat briefings that are specific to the chemical sector.

DHS also is developing the Homeland Security Information Network—Chemical, a secure network for sharing information among DHS, state and local governments, law enforcement, and private sector critical infrastructure, including the chemical industry. Through the network, the chemical industry will receive immediate reports of threats to the sector directly from the Homeland Security Operations Center and DHS chemical sector specialists. The system also will allow owners/operators to report information to the government and each other. The network will allow for collaboration and coordination among chemical sector stakeholders, a

---

<sup>20</sup>The Homeland Security Act and Homeland Security Presidential Directive 7 require DHS to collaborate with the private sector.

<sup>21</sup>The Federal Bureau of Investigation's National Infrastructure Protection Center created ISAC with ACC. The Homeland Security Act transferred these functions to DHS, which now supports ISAC.

---

shared document repository for best practices and planning activities, and forums for discussion. The chemical sector is one of the first sectors to pilot test the new system—approximately 25 industry officials have access to it. DHS plans to eventually enroll in the system all chemical company employees with a need for access to sensitive security information. According to ACC, legal concerns, such as who will operate the system and how DHS will protect the information provided by industry from release under the Freedom of Information Act, have delayed the use of the system. DHS is working with the industry on drafting agreements on the use of the network and information protection.

The Chemical Sector Coordinating Council was formed voluntarily by trade associations within the chemical sector in June 2004, and it currently comprises representatives from 16 key industry stakeholder associations. The council is a single point of contact to facilitate organizing and coordinating sector policy developments, infrastructure protection planning, and plan implementation activities. In addition to serving as a routine information-sharing mechanism, the council has helped DHS develop an emergency response exercise and industry guidance and is working closely with DHS to develop, refine, and disseminate the RAMCAP methodology. Furthermore, DHS provided the council with a draft of its Chemical Sector-Specific Plan for comments in September 2005.

According to DHS, the council represents the majority of chemical facility owners/operators through its broad membership. The council defines the chemical sector as “entities engaged in the production of chemicals, as well as those engaged in the storage, transportation, delivery, and use of chemicals not adequately addressed by other critical infrastructure sectors.” The council does not include water treatment facilities or chemical transportation modes (rail, truck, and barge) since both have separate sector coordination mechanisms. DuPont’s Director of Global Operations Security currently serves as the chair of the council to provide a specific, frontline perspective and guidance. The industry associations participating on the council include the following:

- The Adhesive and Sealant Council
- American Chemistry Council
- American Forest & Paper Association
- Chemical Producers and Distributors Association

- 
- Chlorine Chemistry Council
  - The Chlorine Institute
  - Compressed Gas Association
  - CropLife America
  - The Fertilizer Institute
  - Institute of Makers of Explosives
  - International Institute of Ammonia Refrigeration
  - National Association of Chemical Distributors
  - National Paint and Coatings Association
  - National Petrochemical and Refiners Association
  - The Society of the Plastics Industry, Inc.
  - Synthetic Organic Chemical Manufacturers Association

According to ACC, the interchange between DHS and the council has been hampered by DHS's slow progress in determining whether the Federal Advisory Committee Act (FACA) applies to the council.<sup>22</sup> Among other things, under FACA, federal advisory committee meetings must generally be open to the public, and agencies are required to prepare meeting minutes and make them available to interested parties.<sup>23</sup> The Homeland Security Act allows the Secretary of DHS to establish and use the services of advisory committees and to exempt such committees from FACA.<sup>24</sup> In

---

<sup>22</sup>Pub. L. No. 92-463, 86 Stat. 770 (1972) (classified at 5 U.S.C. app. 2).

<sup>23</sup>The President or head of an agency may determine that a meeting be closed if, for example, the meeting will include discussions of classified information, reviews of proprietary data submitted in support of federal grant applications, or deliberations involving considerations of personal privacy.

<sup>24</sup>If the Secretary exempts a committee from FACA, the Secretary must publish a notice in the *Federal Register* announcing the establishment of an advisory committee and identifying its purpose and membership. See 6 U.S.C. § 451.

---

June 2005, the Homeland Security Advisory Council recommended that the Secretary exempt both Sector Coordinating Councils and ISACs from FACA because of the critical value of this information-sharing relationship.<sup>25</sup>

To share industry best practices, DHS has prepared three guidance documents that highlight common issues across the chemical sector and identify measures for protecting chemical facilities. These reports are (1) the Common Characteristics and Vulnerabilities report, (2) the Potential Indicators of Terrorist Activity report, and (3) the Protective Measures report. DHS has provided copies of these reports to state Homeland Security Offices and the Chemical Sector Coordinating Council for distribution to owners/operators of chemical facilities and the law enforcement community.

DHS also hosts training and tabletop exercises for facility owners/operators; state, local, and tribal governments; and local law enforcement agencies. DHS has developed a number of courses on such topics as surveillance detection, terrorism awareness, and buffer zone protection. DHS has hosted tabletop exercises at six high-risk chemical facilities and invited industry officials to participate in TopOff3, the third in a series of congressionally mandated emergency response exercises. These extensively planned exercises simulate a terrorist attack and test federal, state, local, and private sector responses. Industry officials we spoke with said both government and private sector participants learned valuable lessons from the exercises.

Both DHS and the Homeland Security Advisory Council recognize the challenges in sharing information with the industry. According to department officials, DHS has difficulty reaching all members of the chemical sector. To address this issue, DHS plans to utilize ISAC as well as the Chemical Sector Council, other federal agencies, and state and local authorities to assist in identifying and communicating with chemical facilities. The Homeland Security Advisory Council recently recommended ways to improve information sharing between DHS and the industry.

---

<sup>25</sup>The Homeland Security Advisory Council provides advice and recommendations to the Secretary on matters related to homeland security. The council is comprised of leaders from state and local governments, first responder communities, the private sector, and academia.

---

---

## DHS Coordinates with EPA and Other Federal Agencies

Homeland Security Presidential Directive Number 7 directs DHS to work closely with other federal departments and agencies, state and local governments, and the private sector to identify and prioritize the nation's critical infrastructure and key resources and to protect them from terrorist attacks. DHS coordinates its chemical security efforts with EPA and other federal agencies through a government coordinating council. As outlined in DHS's Interim National Infrastructure Protection Plan, government coordinating councils are intended to include representatives from DHS and the appropriate federal agencies to work with the Sector Coordinating Council in supporting the nation's homeland security mission. According to DHS's 2004 draft Chemical Sector-Specific Plan, DHS views government coordinating councils as the future of sector coordination and communications activities. Participants in the chemical sector government coordinating council include officials from the Department of Commerce's Bureau of Industry and Security; Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives and the Federal Bureau of Investigation; the Department of Transportation's Federal Railroad Administration, Federal Motor Carrier Safety Administration, and Pipeline and Hazardous Materials Safety Administration; and EPA's Office of Emergency Management and Water Security Division. DHS also recently invited officials from the Department of Energy, the Department of Labor's Occupational Safety and Health Administration, and the Department of Defense to participate on the council. As of October 2005, the council had met four times to discuss issues related to chemical sector security. DHS officials told us that recent meetings included discussions of such topics as comparing the work of different government agencies on modeling chlorine incidents.

In addition to interactions through the coordinating council, EPA has provided DHS with a copy of the RMP database and participates on a RAMCAP committee to develop chemical sector tools. According to EPA officials, however, EPA has not played a major role in analyzing these or other data on chemical risks to identify or prioritize chemical facilities. EPA officials believe that the agency could further assist DHS by providing analytical support in identifying high-risk facilities that should be targeted in DHS's chemical sector efforts. These officials also believe that the agency has expertise in a number of other areas that has not been tapped and could support DHS's activities. In addition to EPA's expertise on RMP data and its familiarity with RMP facilities, EPA maintains information on hazardous chemicals and related facilities. For example, EPA collects some information under the Toxic Substances Control Act on industrial chemicals that may pose environmental or human health hazards and collects information about oil and pesticides facilities under other

---

authorities. Furthermore, as the lead federal agency for hazardous materials emergency response, EPA has infrastructure in place around the country with designated on-site coordinators for hazardous materials incidents. These officials, as well as field inspectors who visit chemical facilities under a variety of environmental programs, are familiar with chemical facilities across the country and have general knowledge of process safety issues and expertise on hazardous material releases. EPA officials also told us that EPA staff have garnered extensive knowledge about the chemical sector through informal information sharing about facility practices. For example, EPA officials explained that before the RMP program, EPA collected and shared general information about facility safety problems as well as strategies facilities have used to address these problems. Finally, as the lead agency for the water sector, EPA has developed knowledge on security issues related to drinking water facilities. In this regard, under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, EPA is responsible for receiving vulnerability assessments from community water systems serving more than 3,300 people.

DHS officials believe that their coordination with EPA has been sufficient; they told us that they do not see a need for additional coordination with EPA on data analysis or other efforts because EPA has no expertise relating to chemical industry security matters, as does DHS. Furthermore, the DHS officials stated that EPA is a safety agency and can add little to modeling or analysis of RMP data from a security perspective. DHS officials also told us that the department has not involved EPA in site assistance or Buffer Zone Protection Plan visits at chemical facilities because the owners/operators would strongly oppose EPA's involvement, given its role in regulating other aspects of the chemical industry. These officials explained that, while EPA will be involved in the planning and preparation aspects of DHS's chemical sector Comprehensive Reviews—which will bring together groups of government officials to visit clusters of chemical facilities in specific geographic areas—EPA will not participate in the site visits for the same reason.

---

---

## The Chemical Industry Continues Voluntary Efforts to Address Security, but Faces Challenges in Safeguarding Facilities

The chemical industry, led by its industry associations, has undertaken voluntary efforts to address plant security, but faces challenges in preparing facilities against terrorism. Some industry associations require member companies to assess their facilities' vulnerabilities and make security enhancements. For example, ACC requires, as a condition of membership, that companies conduct vulnerability assessments, develop and implement plans to mitigate vulnerabilities, and have a third party verify that the security enhancements identified in the plans were implemented. Other industry associations have encouraged their members to address security by developing security guidelines, best practices, and other tools. Although the chemical industry has taken these actions, industry officials told us that they face a number of challenges in preparing facilities against a terrorist attack. For example, they reported that the cost of security improvements can be a burden, particularly for smaller companies that may lack the resources larger chemical companies have to devote to security.

---

## Some Industry Associations Require Members to Assess Vulnerabilities and Enhance Security

With few federal security requirements, industry associations have been active in promoting security among member companies. As we reported in March 2005, some industry associations require member companies to assess their facilities' vulnerabilities and make security enhancements, requiring as a condition of membership that they conduct security activities and verify that these actions have been taken.<sup>26</sup> Appendix II includes a description of security efforts that individual industry associations are undertaking.

ACC, representing 135 chemical manufacturing companies with approximately 2,000 facilities, has led the industry's efforts to improve security at their facilities. In 1988, ACC initiated its Responsible Care® Management System, which is a comprehensive management system for its members to follow to continuously improve safety performance; increase communication; and protect employees, communities, and the environment. In June 2002, as part of its Responsible Care® Management System, ACC adopted a security code requiring its members to adhere to a set of security management principles. For physical site security, member companies are to perform vulnerability assessments using an approved methodology. Companies also must develop plans to mitigate

---

<sup>26</sup>GAO-05-327.

---

vulnerabilities, take actions to implement the plans, and have an independent party verify that the facilities implemented the identified physical security enhancements. Third-party reviewers can include insurance representatives, local emergency responders, or local law enforcement officials. These reviewers do not verify that a vulnerability assessment was conducted appropriately or that actions taken by a facility adequately address security risks. However, the Responsible Care® Management System requires member companies to periodically conduct independent third-party audits that include an assessment of their security programs and processes and their implementation of corrective actions. According to ACC, all members have completed their physical security vulnerability assessments and almost all have had their physical security enhancements verified.

The Responsible Care® Security Code also established requirements for cyber assets, such as computer systems that control chemical facility operations, and the distribution chain, which covers the complete “value chain” for chemicals, from suppliers to customers, including transportation. ACC member companies must perform vulnerability assessments of cyber assets and the distribution chain and implement plans to mitigate any vulnerabilities. Examples of security improvements in distribution include measures such as additional screening of transportation providers.

ACC asked each member company to provide a signed statement from a company executive that the company had management systems in place for the entire security code by June 30, 2005. According to ACC, as of October 1, 2005, 95 percent of its member companies affirmed that they had implemented a security management system for physical security, cyber security, and the distribution chain. The Coast Guard recognized the Responsible Care® Security Code as an alternative security program for purposes of fulfilling security requirements under MTSA.

The Synthetic Organic Chemical Manufacturers Association (SOCMA), which includes 160 specialty chemical manufacturers that operate about 300 small- to medium-sized facilities in the United States, also adopted the Responsible Care® Security Code in December 2002.<sup>27</sup> SOCMA developed

---

<sup>27</sup>Specialty chemicals are formulated to meet the detailed specifications of various end users and usually have unique purposes, such as making nylon fibers stronger or serving as the active ingredient in medicine.



---

its own vulnerability assessment methodology that is designed to address the unique needs of its members, which are primarily small businesses. According to SOCMA officials, all of its member companies have reported completing vulnerability assessments, and 98 percent of these companies reported that they had implemented security enhancements and obtained third-party verification, as of September 2005. However, beginning in October 2005, SOCMA no longer required its members to adhere to the Responsible Care® Management System because it has developed its own environmental, health, safety, and security performance program. SOCMA's new program, called ChemStewards<sup>SM</sup>, still requires members to conduct vulnerability assessments for physical security and implement appropriate countermeasures. In addition, facilities that are subject to RMP must have third parties verify implementation of security measures.

Furthermore, the National Association of Chemical Distributors (NACD)—which represents 253 companies with approximately 1,380 facilities in the United States and Canada that package, distribute, and blend chemicals, typically in warehouse facilities—has developed an environment, health, safety, and security management protocol called the Responsible Distribution Process. Created in 1991, adherence to the Responsible Distribution Process is a condition of NACD membership. Since January 1998, NACD members have been required to undergo and successfully complete on-site third-party verification of the company's implementation of all required membership practices once every 3 years. NACD contracted with an internal auditing company to be the third-party reviewer for its members. The first 3-year cycle of Responsible Distribution Process verification ended in December 2001. In April 2002, NACD added security measures to the process that require its members to develop security programs, scrutinize security measures taken by for-hire motor carriers, check that customers are purchasing chemicals for the appropriate use (as prescribed by government regulations), and verify implementation of security measures by an independent firm designated by NACD. The second 3-year cycle for process verification began in January 2003 and will end in December 2005. NACD has terminated the membership of 20 companies that failed to comply with Responsible Distribution Process requirements and to complete and pass third-party verification. Beginning in January 2006, NACD's Responsible Distribution Process includes a requirement that members conduct security vulnerability assessments. Members will be expected to have completed their assessment by June 2006. NACD also developed its own vulnerability assessment methodology specific to its members.

---

---

## Other Industry Associations Have Developed Security Guidelines, Best Practices, and Other Tools

Other industry associations have encouraged their members to address security by a variety of means, rather than only by establishing security requirements that include steps to verify compliance. Most of the associations we spoke with have taken steps to educate their members about security by developing security guidelines and best practices. For example, the Compressed Gas Association, representing 138 companies that manufacture or distribute gases and related products, developed guidance for its members on site security, transportation security, and security steps to check that customers are purchasing gas products for the appropriate uses. The Institute of Makers of Explosives, representing 40 companies of which 30 are explosives manufacturers and distributors, also provided recommended guidelines for security to its members. The guidelines recommend security practices specific to the manufacture, transportation, storage, and use of explosives products and also recommend that facilities conduct vulnerability assessments and develop security plans.<sup>28</sup> In addition, the International Institute of Ammonia Refrigeration, representing facilities such as food storage warehouses, developed site security guidelines tailored to ammonia refrigeration facilities and provides information about security resources to members. All 16 associations we met with told us they keep members apprised of security issues and discuss security at meetings, training courses, and conferences.

In addition to these efforts, several industry associations have developed vulnerability assessment methodologies to assist their member companies in evaluating security needs. For example, the National Petrochemical and Refiners Association, in partnership with the American Petroleum Institute, developed a vulnerability assessment methodology tailored to refineries and petrochemical facilities. The methodology was developed in cooperation with the Department of Energy and DHS and has been approved by the Center for Chemical Process Safety. In addition, an agribusiness working group comprising members of the Agricultural Retailers Association, CropLife America, and the Fertilizer Institute, developed a Web-based security vulnerability assessment tool for agricultural facilities that has also been approved by the Center for Chemical Process Safety. According to the Fertilizer Institute,

---

<sup>28</sup>Explosives companies are regulated by Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives.

---

approximately 2,000 retail agricultural facilities have used the tool to date.<sup>29</sup> Furthermore, the Chlorine Institute, which represents approximately 220 companies involved in the production, distribution, and use of chlorine, developed a seven-step process that smaller chlorine manufacturing and distribution companies can use to assess their vulnerabilities. The process takes companies through a series of steps that score facilities in different areas to identify vulnerabilities. Security experts have reviewed and approved the institute's process.

Some associations also recommend or require that member companies follow security programs, but they do not require steps to verify compliance. The National Paint and Coatings Association, which represents over 300 paint and coatings manufacturing and supply companies, worked with its members to develop a safety and environmental management system called Coatings Care. This system includes security steps such as analyzing threats, vulnerabilities, and consequences and implementing security measures. Member companies have 1 year from the time they join the association to agree to follow Coatings Care principles. However, the association does not require third-party verification of security steps. Similarly, the Chlorine Institute requires executives at all member companies to sign an agreement stating that they will meet nine safety and security requirements, including complying with the Responsible Care® Management System, NACD's Responsible Distribution Process, or another industry security program. While companies that do not sign the agreement are not eligible for Chlorine Institute membership, the institute does not require that companies take steps to verify compliance with security programs. In addition, the Fertilizer Institute, which represents approximately 190 companies that make, sell, or transport fertilizer products, recommends but does not require that members follow a Security Code of Management Practices that involves screening facilities into priority tiers on the basis of potential security hazards and conducting a vulnerability assessment, following a timeline that is based on their tier level.

Despite industry associations' efforts to encourage or require members to voluntarily address security, the extent of participation in the industry's voluntary initiatives is unclear. DHS has not estimated the extent of participation in voluntary initiatives across the chemical sector.

---

<sup>29</sup>The security vulnerability assessment is owned and operated by the Agricultural Retailers Association.

---

Furthermore, not all chemical companies belong to the associations that represent their industry sectors. DHS does not have data on the number of RMP facilities that belong to these associations.

---

## The Chemical Industry Faces Challenges in Securing Facilities against Terrorism

Chemical industry officials told us they face a number of challenges in preparing facilities against a terrorist attack. Most of the chemical associations we contacted stated that the cost of security improvements is a challenge for some chemical companies. Industry officials we spoke with said that some companies have already made significant investments to improve security. For example, ACC reports that its members have spent an estimated \$2 billion on security improvements since September 11, 2001. However, industry associations told us that while some companies have implemented security enhancements, others may not be implementing security measures because of cost concerns. Representatives of the American Forest & Paper Association and the National Paint and Coatings Association told us that small companies, in particular, may struggle with the cost of security improvements or the cost of complying with any potential government security programs because they may lack the resources larger companies have to devote to security.

Many industry officials suggested that federal assistance via grants or tax incentives to offset security costs could help companies enhance facility security. According to these officials, financial incentives to companies to support both vulnerability assessments and security improvements would be helpful. Representatives from two industry associations stated that financial assistance from the government to support the cost of compliance with voluntary programs such as the Responsible Care® Management System would be helpful, noting that complying with voluntary programs is very costly. Other industry officials suggested that DHS direct funding to high-risk facilities it views as vulnerable. A number of officials also told us that financial incentives for security improvements will make chemical security legislation, if enacted, more palatable to industry. In this regard, H.R. 713, introduced in the 109<sup>th</sup> Congress, would create a tax credit for 50 percent of the cost incurred by eligible agricultural businesses for protecting hazardous chemicals or pesticides from unauthorized access.

Industry stakeholders also cited the need for guidance on what level of security is adequate. While DHS has issued guidance to state Homeland Security Offices and the Chemical Sector Coordinating Council on vulnerabilities and protective measures that are common to most chemical facilities, several stakeholders expressed a desire for guidance on specific

---

security improvements. For example, representatives of the National Petrochemical and Refiners Association stated that one reason the association holds workshops and best practices sessions is to meet the challenge of determining the types of security measures that constitute a reasonable amount of security. Another association stated that standardized security criteria would be useful in helping companies determine adequate levels of security. In addition, a number of associations told us that companies are operating on tight profit margins and want to feel certain that the benefits of security improvements justify the cost. According to these associations, while companies are addressing security since the events of September 11, 2001, they have to make cost-effective decisions about allocating their resources. Because it is unlikely that sufficient resources will be available for companies to address all risks, adopting a risk management framework can aid facilities in prioritizing risks and the actions taken to reduce those risks, taking cost into consideration.<sup>30</sup>

In addition, industry officials told us that the lack of threat information makes it difficult for companies to know how to protect facilities. Two associations told us that ISAC has not been very useful to members because the information shared is not new or is very broad. Some officials have attended classified briefings with DHS but reported that very little specific information was provided. Other industry association officials told us that DHS has withheld some threat information because it was classified. Providing both classified and declassified or sanitized information to associations would allow them to understand specific threats and pass on unclassified information to members. An official with an agricultural chemical company told us that many companies do not have access to threat information applicable to rural areas that may have different threats than companies located in urban areas. While companies would like to receive very specific threat information, some officials acknowledged that such information may not exist. Officials with one association hoped that DHS's Homeland Security Information Network will improve the quality of the threat information that DHS shares with industry.

---

<sup>30</sup>A risk management framework represents a series of analytical and managerial steps, basically sequential, that can be used to assess risk, assess alternatives for reducing risks, choose among those alternatives, implement the alternatives, monitor their implementation, and continually use new information to adjust and revise the assessments and actions, as needed.

---

A few industry officials also mentioned limited guidance on conducting vulnerability assessments and difficulty in conducting employee background checks as challenges. One industry association stated that it would like its members to receive guidance from DHS on how to conduct vulnerability assessments. Another association expressed frustration because none of the current vulnerability assessment tools address issues specific to its members' facilities, which package and distribute chemicals, and it would like DHS to help develop or approve a methodology for this type of facility. Furthermore, representatives of forest and paper products companies reported that the inaccessibility of government records has made conducting background checks on employees difficult. Officials told us that in addition to regular facility employees, the number of contractors continuously moving through facilities could pose security risks without the appropriate background checks. Access to employment and criminal records would allow facility officials to conduct a more thorough check on employees, thereby reducing the risk of hiring someone who could threaten a facility.

Finally, a number of stakeholders we contacted told us that emergency response preparedness is a challenge for chemical companies. An official with an industry-affiliated research center asserted that emergency responders and communities in the United States are prepared to respond to a toxic release. However, other stakeholders we spoke with stated that many facilities have conducted security vulnerability assessments but may not have done enough emergency response planning and outreach to the responders and communities that would be involved in a release. A 2004 survey by a chemical workers union of workers at 189 RMP facilities found that only 38 percent of respondents indicated that their companies' actions in preparing to respond to a terrorist attack were effective, and 28 percent reported that no employees at their facilities had received training about responding to a terrorist attack since September 11, 2001.<sup>31</sup> While environmental laws require emergency response planning for accidental chemical releases, several stakeholders told us facilities need to consider very different scenarios with consequences on different orders of magnitude when planning the emergency response for a terrorist incident. An expert with Texas A&M University's National Emergency Response and Rescue Training Center echoed this view, noting that chemical facility

---

<sup>31</sup>Paper, Allied-Industrial, Chemical, and Energy Workers International Union, *PACE International Union Survey: Workplace Incident Prevention and Response Since 9/11* (October 2004).

---

employees are well-trained for an accidental release but may not be trained in the emergency response for a terrorist release. According to this expert, both facility employees and local emergency responders need to prepare for terrorist-caused chemical releases that are less predictable and harder to prepare for than accidental releases. Facilities should be aware of the types of aid located within a 50-mile radius of the facility, such as welders, neutralizing chemicals, and back-up protection equipment, according to this expert. While some companies have formed mutual-aid groups in a given geographic area, the expert cautioned that these groups may not prove effective if facilities lock down and focus on protecting themselves when terrorists attack.

---

## **DHS Needs Additional Authority to Ensure That Chemical Facilities Are Addressing Security Issues**

Existing laws provide DHS with only limited authority to address security concerns at U.S. chemical facilities, and additional legislation is needed to place federal security requirements on these facilities. DHS lacks the authority to require all high-risk chemical facilities to assess their vulnerabilities and implement security measures and, consequently, has relied largely on the industry's voluntary participation to address facility security. As a result, DHS cannot ensure that facilities are assessing their vulnerability to terrorist attacks and taking corrective actions, where necessary. DHS has acknowledged that its existing authorities do not permit it to effectively regulate the industry, and that the Congress should enact federal security requirements for chemical facilities. Furthermore, we concluded in 2003, and continue to believe, that additional legislation is needed. Although many stakeholders agreed on the need for federal requirements, they had mixed views on the content and structure of such requirements. They also identified a number of challenges the federal government will face in implementing chemical security requirements.

---

## **Existing Laws Give DHS Limited Authority to Address Chemical Sector Security, but Specific Authority Is Needed to Require All High-Risk Facilities to Act**

A number of existing laws outline DHS's responsibilities for coordinating with the private sector and obtaining information on and protecting critical infrastructure. While the chemical industry is included in the nation's critical infrastructure, these laws provide DHS with only limited authority to address security concerns at U.S. chemical facilities.

---

The Homeland Security Act assigns DHS responsibility for coordinating and collaborating with the private sector on certain homeland security issues. Under the Homeland Security Act, the Secretary of DHS is responsible for coordinating homeland security issues with the private sector to ensure adequate planning, equipment, training, and exercise activities. The Homeland Security Act also makes the Special Assistant to the Secretary (Private Sector) responsible for (1) promoting and developing public-private partnerships for collaboration and mutual support to address homeland security challenges, (2) assisting in promoting and developing private sector best practices to secure critical infrastructure, and (3) coordinating industry efforts to identify private sector resources and capabilities that could effectively supplement government efforts to prevent or respond to a terrorist attack.<sup>32</sup>

Existing laws also assign DHS responsibilities specifically related to the protection of critical infrastructure, including chemical facilities. The Patriot Act called for the establishment of the National Infrastructure Simulation and Analysis Center (NISAC)—a partnership between Los Alamos and Sandia National Laboratories—under DHS to help protect critical infrastructure by supporting counterterrorism, threat assessment, and risk mitigation activities.<sup>33</sup> NISAC is to provide support—such as modeling, simulation, and analysis of critical infrastructure systems—to facilitate modifying these systems to mitigate threats to them and to critical infrastructure in general. In addition, the Homeland Security Act gives DHS’s Under Secretary for Information Analysis and Infrastructure Protection (IAIP) responsibilities related to protecting critical infrastructure, including

- accessing, receiving, analyzing, and integrating information from federal, state, and local governments and private sector entities to identify, detect, and assess the nature and scope of terrorist threats to

---

<sup>32</sup>All standards activities are to be conducted in conformance with section 12(d) of the National Technology Transfer Act of 1995, which states that federal agencies generally must use technical standards—performance-based or design-specific technical specifications and related management systems practices—developed or adopted by voluntary consensus standards bodies as a means to carry out policy objectives or activities, consulting and participating with such bodies in the development of technical standards when such participation is in the public interest and compatible with the agency’s authorities and budget resources. See 6 U.S.C. §112(g) and 15 U.S.C. § 272 note.

<sup>33</sup>Pub. L. No. 107-56, § 1016, 115 Stat. 400 (2001) (codified at 42 U.S.C. § 5195c(d)).



---

the United States, and to understand these threats in light of actual and potential vulnerabilities;

- carrying out comprehensive assessments of the vulnerabilities of the nation's key resources and critical infrastructure, including assessing the risks posed by particular types of terrorist attacks within the United States, the probability of success of such attacks, and the feasibility and potential efficacy of various countermeasures to such attacks;
- developing a comprehensive national plan for securing the nation's key resources and critical infrastructure; and
- recommending the necessary measures to protect these key resources and critical infrastructure.

While DHS's existing legal authorities provide it with access to some information about critical infrastructure threats and vulnerabilities, DHS does not have the authority to require all chemical facilities to conduct vulnerability assessments.<sup>34</sup> The Homeland Security Act provides DHS with access to all information that may be collected, prepared, or possessed by any federal agency concerning infrastructure or other vulnerabilities of the United States to terrorism. Under the Homeland Security Act, DHS may request information from the private sector through cooperative agreements. In addition, the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRRA) required the Attorney General to review and report on the vulnerability of certain chemical facilities to criminal and terrorist activity and current industry practices regarding site security.<sup>35</sup> In 2003, \$3 million was transferred from Justice's general administration appropriation to DHS as part of the Consolidated Appropriations Resolution, 2003, and the conferees stated that they expected DHS to use the transferred funds to conduct the vulnerability assessments under CSISSFRRRA.<sup>36</sup> However, CSISSFRRRA does not give DHS

---

<sup>34</sup>Under MTSA, DHS's Coast Guard requires maritime facility owners/operators to conduct assessments of vulnerabilities, develop security plans, and implement security measures. The Coast Guard also has the authority to enter facilities. However, the Coast Guard reports that these requirements currently apply to only 300 chemical facilities.

<sup>35</sup>Pub. L. No. 106-40, § 3(a) (1999). Justice partially fulfilled this requirement by submitting an interim report on the vulnerability of chemical facilities in May 2002. Neither Justice nor DHS has submitted a final report to the Congress, which was due on August 5, 2002.

<sup>36</sup>H.R. Conf. Rep. No. 108-10 (2003).

---

the authority to require facilities to conduct vulnerability assessments. Similarly, the October 2004 conference report on DHS's fiscal year 2005 appropriations act directed IAIP—within DHS—to analyze whether DHS should require private sector entities to provide IAIP with existing information about their security measures and vulnerabilities in order to improve its ability to evaluate critical infrastructure protection nationwide. The conference report stated that the analysis should include all critical infrastructure, including chemical plants, and evaluate the benefits of securing the information and the costs to both the private sector and IAIP for implementing this requirement.<sup>37</sup> However, neither the appropriations act nor any other legislation would require chemical facilities to provide information about their security and vulnerabilities.

Furthermore, DHS currently lacks the authority to enter all chemical facilities without their permission to assess security or to require and enforce security improvements. In this regard, except with respect to certain chemical facilities covered under federal security requirements for other critical infrastructures, existing laws do not give DHS the right to enter a chemical facility to assess its vulnerability to a terrorist attack or the authority to require and enforce the implementation of any needed security improvements at these facilities. The Homeland Security Act, with some limited exceptions, does not provide any new regulatory authority to DHS and only transferred the existing regulatory authority of any agency, program, or function transferred to DHS, thereby limiting actions DHS might otherwise be able to take under the Homeland Security Act.<sup>38</sup> Therefore, DHS has relied solely on the voluntary participation of the private sector to address facility security. As a result, DHS cannot ensure that all high-risk facilities are assessing their vulnerability to terrorist attacks and taking corrective action, where necessary.

In contrast, some other critical infrastructure sectors are subject to federal security requirements. For example, all commercial nuclear power plants licensed by the Nuclear Regulatory Commission are required to take security steps, including placing physical barriers outside of the operating reactor area, limiting access to vital areas, and maintaining a trained

---

<sup>37</sup>H.R. Conf. Rep. No. 108-774, at 75 (2004).

<sup>38</sup>The Secretary may issue regulations for antiterrorism technology and may issue necessary regulations with respect to research; development; demonstration; testing; and evaluation activities of the department, including the conducting, reviewing, and funding of such activities.

security force. In addition, community water systems that serve more than 3,300 people are required to conduct and submit a vulnerability assessment to EPA and prepare an emergency response plan that incorporates the results of the assessment. Table 3 provides examples of federal security requirements that are in place for these and some other critical infrastructure sectors.

**Table 3: Examples of Federal Security Requirements for Other Critical Infrastructure Sectors**

Sector	Public law or other requirement	Major provisions
Aviation	Aviation and Transportation Security Act of 2002	This act created the Transportation Security Administration, now within DHS, to assume responsibility for aviation security, including the screening of passengers and their baggage.
Drinking water	Public Health Security and Bioterrorism Preparedness and Response Act of 2002	Community water systems serving more than 3,300 people are required to assess the system's vulnerability to terrorist attacks, prepare an emergency response plan that incorporates the results of this assessment, certify to EPA that the assessment and response plan have been completed, and provide a copy of the assessment to EPA. According to EPA, 1,928 drinking water facilities that are also subject to EPA's RMP program must comply with this act.
Food	Public Health Security and Bioterrorism Preparedness and Response Act of 2002	This act requires all domestic and foreign facilities that manufacture, process, pack, or hold food for human or animal consumption in the United States to register with the Food and Drug Administration (FDA) by December 12, 2003. Restaurants, certain retail stores, nonprofit feeding establishments, fishing vessels, and farms are exempt from these registration requirements. FDA is also to give high priority in increasing the number of inspections of food offered for import at ports of entry into the United States, with the greatest priority given to inspections to detect the intentional adulteration of food.
Nuclear	Nuclear Regulatory Commission advisories and orders	Commercial nuclear plants licensed by the Nuclear Regulatory Commission are required to take security steps such as placing physical barriers outside reactor areas, limiting access to vital areas, maintaining a trained security force, and conducting simulated terrorist attack exercises.
Ports	Maritime Transportation Security Act of 2002	Maritime facility owners and operators must conduct vulnerability assessments, develop security plans, and implement the measures discussed in security plans. The Coast Guard conducts inspections at these facilities, and MTSA prohibits operation of facilities that do not have the required security plans or that are not operating in compliance with these plans. The Coast Guard has reviewed and approved facility security plans for 238 chemical facilities.

Source: GAO.

---

---

## DHS Has Concluded That It Needs Additional Authority to Address Chemical Facility Security

DHS has concluded that its existing patchwork of authorities does not permit it to regulate the chemical industry effectively, and that the Congress should enact federal requirements for chemical facilities. While DHS reports that most chemical companies have been eager to voluntarily cooperate with agency efforts to address security issues at their facilities, DHS determined that voluntary efforts alone will not sufficiently address security for the entire sector. Echoing public statements by the Secretary of DHS and the Administrator of EPA in 2002 that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness, in June 2005, both DHS and EPA called for legislation to give the federal government greater authority over chemical facility security.<sup>39</sup> Similarly, we concluded in 2003, and continue to believe, that additional federal legislation is needed because of the significant risks posed by thousands of chemical facilities across the country to millions of Americans and because the extent of security preparedness at these facilities is unknown.<sup>40</sup>

In testimony before the Congress in June 2005, the Acting Undersecretary for IAIP stated that any proposed regulatory structure (1) must recognize that not all facilities within the chemical sector present the same level of risk, and that the most scrutiny should be focused on those facilities that, if attacked, could endanger the greatest number of lives, have the greatest impact on the economy, or present other significant risks; (2) should be based on reasonable, clear, equitable, and measurable performance standards; and (3) should recognize the progress that responsible companies have made to date. He also stated that the performance standards should be enforceable and based on the types and severity of potential risks posed by terrorists, and that facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those risks. In addition, he said that DHS would need the ability to audit vulnerability assessment activities and a mechanism to ensure compliance with requirements.

Beyond these general principles, DHS officials were reluctant to share with us their views on the specific content and structure of chemical security legislation. These officials explained that DHS provides its views on

---

<sup>39</sup>Testimony before the House Homeland Security Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity and the Senate Committee on Homeland Security and Governmental Affairs on June 15, 2005.

<sup>40</sup>GAO-03-439.

---

proposed legislation to the Office of Management and Budget (OMB) as part of the executive branch coordination process, and that OMB—after considering the points of view of all departments, agencies, and independent operating entities—establishes the unified executive branch position on proposed legislation. Because the administration’s unified position had not yet been determined at the time of our discussion, DHS officials believed that it was inappropriate to discuss their views on the specific provisions of any legislation.

---

### Stakeholders’ Views on Chemical Security Legislation Are Mixed

While many stakeholders—including representatives from industry, research centers, and government—agreed on the need for additional legislation that would place federal security requirements on chemical facilities, they had mixed views on the content and structure of such requirements. Representatives of three research organizations and three environmental groups told us that DHS needs more authority to adequately ensure that chemical facilities are taking action, based on the potential harm that an attack on chemical facilities may cause. One expert stated that chemical facility security is a public safety issue that warrants federal oversight, while others said the number of facilities with potential off-site consequences in proximity to population centers justifies federal involvement in security. Furthermore, testifying in support of legislation before the Congress in July 2005, a representative of a chemical workers union underscored that workers and communities should not be placed at risk because some companies choose not to prioritize security and that, in the same vein, responsible companies should not be placed at an economic disadvantage because they allocate resources to security. Half of the industry associations we contacted also favor additional legislative authority. ACC has publicly stated that they support chemical security legislation for a number of reasons, including the belief that all of the nation’s chemical facilities should be required to take the security steps that its members are taking under the Responsible Care® Management System. One association supported federal legislation because its members are encountering various state efforts to oversee facility security. Concerned that member companies will be subject to different security requirements in different states, officials with three associations would rather the federal government take the lead on chemical facility security.

Other stakeholders preferred that DHS continue to work with the industry to voluntarily address security or were undecided about the need for federal requirements. Two industry associations stated that the partnership DHS has forged with the chemical industry has proven effective in working

---

to address security concerns. In July 2005 testimony before the Congress, the National Petrochemical and Refiners Association expressed concern that legislation giving DHS authority over chemical facility security will negatively impact the cooperative relationship the industry and DHS have established, noting that the level of information sharing could be diminished if DHS becomes an industry regulator. Similarly, two research centers affiliated with the industry did not advocate chemical security legislation. One expressed concern that the goodwill that the industry has shown to DHS will wane if DHS becomes a regulatory agency, while another noted that the threat of new security regulations provides an adequate incentive for facilities to take security steps. Notwithstanding ACC's position, most of the individual chemical companies we contacted also believed that legislation is not needed, or they were undecided about whether DHS needed additional authority. Company officials generally told us that industry self-regulation is preferable to federal oversight of facility security. One company official also told us that states are better suited to regulating facility security because they have greater knowledge about facilities in their state.

Stakeholders expressed a range of views about which facilities should be covered if legislation is enacted; about whether legislation should address inherently safer technologies; about EPA's role, if any; and about voluntary industry programs. Stakeholders favoring legislation generally agreed that legislation should target high-risk facilities, rather than applying the same requirements to all facilities regardless of the different risks they pose. These stakeholders told us that chemical facilities should be prioritized on the basis of their potential impacts if attacked, with the highest-risk facilities subject to stricter requirements than lower-risk facilities that do not warrant the same degree of federal oversight. For example, in testimony before the Senate Committee on Homeland Security and Governmental Affairs in July 2005, ACC explained that any regulatory system must reflect the different risks posed by different facilities and require security measures commensurate with those risks. At the same hearing, a representative of SOCMA, which represents specialty chemical manufacturers, recommended that legislation require facilities to perform a risk screen on the basis of the potential consequences of an attack and the attractiveness as a target. Facilities screened as high risk would then perform a detailed vulnerability analysis. Representatives from two research centers and two companies believed that RMP facilities provide a good starting point for the universe of facilities that legislation should cover because these facilities exceed a risk threshold on the basis of the type and amount of chemicals they house. One company suggested that

---

chemical security legislation should require an analysis of RMP facilities that ranks facilities on the basis of risk.

Stakeholders expressed strongly divergent views on whether legislation should require the substitution of safer chemicals and processes, referred to as “inherently safer technologies.” Implementing inherently safer technologies could potentially lessen the consequences of an attack by reducing the chemical risks present at facilities. Justice, in introducing a methodology to assess chemical facilities’ vulnerabilities, recognized that reducing the quantity of hazardous material may make facilities less attractive to terrorist attack and reduce the severity of an attack. Furthermore, DHS’s July 2004 draft Chemical Sector-Specific Plan states that inherently safer chemistry and engineering practices can prevent or delay a terrorist incident, noting that it is important to make sure that facility owners/operators consider alternate ways to reduce risk, such as inherently safer design, implementing just-in-time manufacturing, or replacing high-risk chemicals with safer alternatives. However, DHS told us that the use of inherently safer technologies tends to shift risks rather than eliminate risks, often with unintended consequences. Some previous chemical security legislative proposals have included a requirement that facility security plans include safer design and maintenance actions, or that facility security plans include “consideration” of alternative approaches regarding safer design. Representatives from three environmental groups told us that facilities have defined security too narrowly as guns, gates, and guards, without focusing on reducing facility risks through safer technologies. Noting that no existing laws require facilities to analyze inherently safer options, these representatives believe legislation should require such an analysis and give DHS or EPA the authority to require the implementation of technologies if high-risk facilities are not doing so. Process safety experts at one research organization recognized that reducing facility hazards and the potential consequences of chemical releases makes facilities less vulnerable to attack. However, these experts also explained that inherently safer technologies can be prohibitively expensive and can shift risks onto other facilities or the transportation sector. For example, reducing the amount of chemicals stored at a facility may increase reliance on rail or truck shipments of chemicals. These experts support legislative provisions requiring analysis or consideration of technology options but do not support giving the federal government the authority to require specific technology changes because of the complexity of these decisions. Representatives of two research centers affiliated with the industry told us that while facilities should look at inherently safer

---

technologies when assessing their vulnerability to terrorist attack, safer technologies are not a substitute for security.

Industry associations and company officials voiced strong opposition to any inherently safer technologies requirements. The majority of the industry officials we contacted opposed an inherently safer technologies requirement, with many stating that inherently safer technologies involve a safety issue that is unrelated to facility security. Industry officials voiced concerns about the federal government's second-guessing complex safety decisions made by facility process safety engineers. Representatives from four associations and two companies told us that, in many cases, it is not feasible to substitute safer chemicals or change to safer processes. Certain hazardous chemicals may be essential to necessary chemical processes, while changing chemical processes may require new chemicals that carry different risks. In July 2005 testimony before the Congress, a SOCMA representative explained that while inherently safer technologies are intended to reduce the overall risks at a facility, this could be achieved only if a chemical hazard was not displaced to another time or location or did not magnify another hazard. Furthermore, process safety experts and representatives from associations and companies report that some safer alternatives are extremely expensive. For example, reducing facility chemical inventories by moving to on-site manufacturing when chemicals are needed can cost millions of dollars, according to a stakeholder. One company also voiced opposition even to a legislative requirement that facilities "consider" safer options. The official explained that the company opposed such a provision—even if legislation does not explicitly give the government the authority to require implementation of safer technologies—because it might leave companies liable for an accident that might have been prevented by a technology option that was considered but not implemented.

Stakeholder views also varied on whether EPA should play a role in developing or enforcing security requirements. Many of the stakeholders we contacted acknowledged that EPA has considerable expertise on chemical facilities, although some noted that DHS lacks expertise specific to the risks related to the chemicals and processes used at facilities. Some of the experts we spoke with stated that EPA should be involved in enforcing any security requirements because of the agency's expertise and because it has an established field presence. Process safety experts also suggested that DHS should work with EPA in identifying the chemicals of concern that would determine which facilities are subject to chemical security requirements. In contrast, all of the industry stakeholders we



---

spoke with about this issue believed that EPA should not have a prominent role, if any, in chemical security legislation because of EPA's regulatory function and because it lacks security expertise. One association said it would be extremely difficult for its members to work with EPA on security issues because the agency's focus on enforcement of environmental regulations would undermine security discussions. Another association was concerned that EPA would approach facility security as an opportunity for further environmental regulation.

Finally, a number of stakeholders believed that any legislation should include provisions recognizing compliance with industry initiatives, such as ACC's Responsible Care® Security Code, equivalent to federal security requirements. Representatives from ACC, SOCMA, the National Association of Chemical Distributors, and other associations underscored that legislation, if enacted, should recognize voluntary industry security programs so facilities that have acted to address security do not have to duplicate efforts they have made to date. In testimony before the Senate Homeland Security and Governmental Affairs Committee in July 2005, an ACC official emphasized the need for legislation to give credit for the substantial voluntary expenditures ACC members have made implementing the Responsible Care® Security Code. Representatives of three environmental groups were not opposed to a provision making compliance with the industry's currently voluntary security programs equivalent to federal requirements, but they emphasized that these facilities should be required to submit documentation of security steps for review by the federal government. The Coast Guard, in implementing MTSA, approved ACC's Responsible Care® Security Code and others as accepted alternative security programs for the purposes of fulfilling security requirements under MTSA.<sup>41</sup> A number of the industry officials we interviewed praised MTSA as a model for chemical security legislation because it allows participation in industry security programs to meet security requirements, and because MTSA's requirements are performance-based rather than prescribing specific actions that all facilities must take. Some industry officials have suggested that legislation should also exempt MTSA-covered chemical facilities from security requirements.

---

<sup>41</sup>These facilities are subject to Coast Guard inspections.

---

---

## Stakeholders Identified Challenges DHS Will Face in Implementing Chemical Security Requirements

Stakeholders identified a number of challenges DHS will face in implementing chemical security requirements. First, some stakeholders told us that identifying the appropriate universe of facilities to be covered by requirements will be difficult, given the diversity of facilities that handle hazardous materials. While the RMP program identifies facilities with amounts of chemicals deemed hazardous to human health, stakeholders told us non-RMP facilities may also need to be considered. For example, process safety experts mentioned that some chemicals not on the RMP list may need to be considered when identifying facilities, such as reactive chemicals that are currently not included under RMP. New Jersey officials noted that the state's chemical security efforts use criteria to identify facilities that exceed RMP criteria, including facilities with RMP chemicals below RMP threshold quantities and non-RMP chemicals that the state deemed hazardous. Representatives from two agricultural chemical companies stated that DHS will have a hard time identifying agricultural facilities that house chemicals of concern, since these facilities range from large plants to small rural facilities. Other stakeholders stated that some RMP facilities should be excluded from security requirements. Representatives of the ammonia refrigeration and forest products industries stated that many of these facilities are not high risk in terms of the possible terrorist threat they pose, even though they are subject to RMP. Officials with two industry associations said that RMP data are not the best indicator of terrorism risks, and that DHS will need to look beyond RMP data to understand the complexities of the chemical sector and identify those facilities with the greatest off-site consequences under terrorist scenarios.

Second, because some states have established their own chemical security requirements, some stakeholders also were concerned about potentially overlapping state and federal requirements. Representatives from two industry associations stressed that the federal government needs to assert its leadership over the chemical sector because states are stepping in where they see a void. At least two states have passed chemical security legislation. Maryland's Hazardous Material Security Act requires RMP facilities in the state to perform vulnerability assessments, develop and implement security measures, and report to the state Department of the Environment. Under New York's Anti-Terrorism Preparedness Act of 2004, the state Office of Homeland Security, subject to available appropriations, must require certain chemical facilities to conduct vulnerability assessments. Stakeholders report that other states have created chemical security offices or are developing chemical security initiatives. Officials with one industry association told us that state homeland security agencies

---

are getting involved in chemical facility security, even though they may lack the resources to fully understand the issues these facilities face. Furthermore, officials with three associations told us that many companies have operations in multiple states and that cooperating with numerous potentially conflicting state efforts would be a burden. Industry officials also said that federal legislation would need to clearly preempt state requirements in order for companies to avoid being subjected to both federal and state laws. State officials from New Jersey and Texas also voiced concern about duplicating efforts with the federal government. State officials from New Jersey, which has used existing state environmental authorities and a state homeland security task force to work with chemical facilities on security issues, suggested that federal legislation would provide industry with a reasonable and predictable set of standards, rather than a patchwork of state requirements. New Jersey officials also told us that although states have done their best to address security concerns, many states, including New Jersey, lack specific enforcement authority that could be provided for in federal legislation.

Third, some stakeholders told us that enforcing chemical security requirements, if enacted, will be a challenge for DHS. While legislation may include enforcement provisions, stakeholders believe DHS may face challenges in implementing any such provisions. Several stakeholders questioned whether DHS has the expertise and resources to enforce security requirements at chemical facilities. New Jersey state officials believe that because DHS lacks experience in dealing with chemical facilities, it should delegate implementation and enforcement authority to states, allowing states to review facility activities and report back to DHS. Unlike the Coast Guard, which conducts facility inspections under MTSA, DHS currently does not have significant staff resources located throughout the country.<sup>42</sup> Some stakeholders suggested that DHS will need staff in the field or will need contract support to enforce requirements. Representatives from two industry associations suggested that allocating federal resources to support chemical facility security preparedness will be a challenge.

Finally, some stakeholders were concerned about the federal government's ability to protect information on facility vulnerabilities and security. Most of the industry associations and company officials we spoke with raised

---

<sup>42</sup>DHS has begun to establish a field presence through the hiring and placement of 63 protective security advisors in metropolitan areas across the country.

---

concerns about this issue, noting that information about facility vulnerabilities and security measures could provide a roadmap for terrorists. While the industry wants to cooperate with DHS on its chemical security efforts, businesses are concerned that sensitive information could be released. This concern arises from the conflict between the public's "right-to-know" such information and security concerns about releasing facility data. As an example, while federal regulations authorized the posting of some RMP data on the Internet and in government reading rooms, some industry officials opposed making this information available. Following the events of September 11, 2001, various media reports published RMP data on some facilities. Industry officials are willing to share information with DHS about the vulnerability assessment process and procedures, but they would prefer that vulnerability and security information remain at the facility, where government officials can view such information if needed. Reporting concerns about DHS's Protected Critical Infrastructure Information (PCII) Program, officials with four associations said companies need additional information about DHS's information protection procedures. Officials with one association added that companies may not be comfortable with the PCII program until it is tested in court. Officials with three industry associations also told us that sharing information at the state level is a concern. In this regard, New Jersey officials noted that they have faced a challenge in allaying industry fears about sharing security information. These officials told us that while some states do not have the ability to protect critical infrastructure information, New Jersey state law exempts private sector information provided for domestic security purposes from open records requirements. In contrast to these views, representatives of three environmental groups believe that some information about high-risk facilities should be publicly available. Specifically, these representatives stated that communities need to understand the risks posed by facilities in the area, and should have access to information on the potential impacts of high-risk facilities' worst-case terrorist scenarios. These representatives told us that details about specific facility vulnerabilities need not be released, but that the public should have access to information about facilities that present the greatest concern.

---

## Conclusions

Across the nation, thousands of facilities produce, use, or store hazardous chemicals in quantities that could potentially put large numbers of Americans at risk. DHS, Justice, and other experts have warned that these facilities present an attractive target for terrorists. A terrorist attack could threaten human health and safety, cause economic disruptions, and impact

---

other critical infrastructures that rely on chemicals. However, the extent of security preparedness at these facilities remains largely unknown. Chemical industry associations have undertaken numerous initiatives to raise awareness about security and to encourage—and in some cases require—member companies to assess their vulnerabilities and act to address them. While these efforts are laudable, participation in these initiatives is voluntary and the extent to which individual companies across the industry are addressing security issues is unclear. Furthermore, voluntary efforts cannot ensure widespread participation and, unless chemical facilities' vulnerabilities are identified and addressed on a widespread basis across the sector, the security of the chemical industry as a critical national infrastructure remains at risk. As the lead federal agency for the chemical sector, DHS has developed a number of programs to assist companies in protecting their chemical facilities. However, unlike other federal agencies—such as EPA and the Nuclear Regulatory Commission, which require drinking water and nuclear facilities, respectively, to take actions to improve their security—DHS does not currently have the authority to require the chemical industry to take such actions. On this basis, DHS has concluded—as we did in 2003—that its existing patchwork of authorities does not allow it to effectively regulate chemical sector security. Since 2002, both DHS and EPA have called for legislation creating security requirements at chemical facilities, and legislation has been introduced in every Congress since the events of September 11, 2001. Our work demonstrates the need to enhance DHS's ability to collect information about industry preparedness and to ensure that facilities evaluate and mitigate their vulnerability to terrorist attack. By granting DHS the authority to require high-risk chemical facilities to take security actions, policy makers can better ensure the preparedness of the chemical sector.

Among its activities to enhance chemical sector security, DHS has developed methods for identifying high-priority facilities, assessing facility vulnerabilities, and suggesting improvements to address these vulnerabilities. In this process, DHS should take full advantage of EPA's expertise on toxic chemical data sources, U.S. hazardous materials facilities, and process safety issues, among other things, that the agency has developed through its oversight of a number of chemical safety programs. For example, EPA maintains data on RMP facilities' inventories of toxic and flammable chemicals and facility worst-case release scenarios and enforces compliance with a variety of environmental programs through inspections of facilities located throughout the country. By tapping EPA's expertise on chemical facilities and general facility safety issues, DHS can

---

enhance its efforts to identify high-priority facilities and assess facility vulnerabilities as well as better target government resources to those facilities posing the greatest risk.

Implementing inherently safer technologies potentially could lessen the consequences of a terrorist attack by reducing the chemical risks present at facilities, thereby making facilities less attractive targets. However, substituting safer technologies can be prohibitively expensive for some companies and can shift risks onto other facilities or the transportation sector. Also, in many cases, it may not be feasible to substitute safer chemicals or change to safer processes. Therefore, given the possible security and safety benefits as well as the potential costs to some companies of substituting safer technologies, a collaborative study employing DHS's security expertise and EPA's chemical expertise could help policy makers determine the appropriate role of safer technologies in facility security efforts.

---

## Matters for Congressional Consideration

To enhance DHS's ability to collect comprehensive information on industry preparedness and better ensure the security of the chemical sector, we recommend that the Congress consider the following two actions:

- granting DHS the authority to require high-risk chemical facilities to assess their vulnerability to terrorist attacks and, where necessary, to take corrective action and
- providing DHS with the enforcement capability to ensure that facilities are following these practices.

---

## Recommendations for Executive Action

Because completion of the Chemical Sector-Specific Plan is critical to DHS's efforts to enhance chemical facility security, we recommend that the Secretary of the Department of Homeland Security direct DHS to take the following two actions:

- ensure that the Chemical Sector-Specific Plan is completed in a timely manner and
- recognizing EPA's expertise in managing chemical risks, jointly study with EPA whether chemical facilities' efforts to reduce vulnerabilities

---

would benefit from the use of technologies that substitute safer chemicals and processes, referred to as “inherently safer technologies.”

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS and EPA for their review and comment. EPA provided no comments on the draft report. DHS agreed in substance with two of the report’s recommendations, but disagreed with the third. DHS agreed that the Congress should consider granting DHS the authority to require the chemical industry to address plant security. DHS also agreed that completing and implementing the sector-specific plan is a priority and stated that it is making progress toward developing this plan. However, DHS disagreed with our recommendation that the department work with EPA to study the security benefits to chemical plants of using safer technologies. In this regard, DHS believes that the use of safer technologies would not generally result in more secure chemical facilities and would tend to shift risks rather than eliminate them. DHS stated that it is unclear what role EPA would play in a study of the benefits of using safer technologies or how DHS’s interaction with EPA might be perceived among DHS’s private sector partners.

We continue to believe, however, that the use of safer technologies may have the potential to reduce security risks for at least some chemical facilities by making them less attractive to a terrorist attack and reducing the severity of the potential consequences of an attack. While we recognize in our report that inherently safer technologies can shift risks onto other facilities or the transportation sector, there may also be instances where implementing safer technologies could reduce the likelihood and severity of a terrorist attack. In fact, DHS’s July 2004 draft of the Chemical Sector-Specific Plan states that inherently safer chemistry and engineering practices can prevent or delay a terrorist incident. The draft also notes that it is important to make sure that facility owners/operators consider alternate ways to reduce risk, such as inherently safer design, implementing just-in-time manufacturing, or replacing high-risk chemicals with safer alternatives. Therefore, we continue to believe that studying the costs and security benefits of using safer technologies would be a worthwhile effort. While DHS, as the federal agency primarily responsible for chemical facility security, should have the lead role in conducting such a study, EPA—charged with ensuring environmental and human health and safety and having the key expertise needed to analyze the potential environmental and health effects of a variety of alternative technologies—can provide valuable support. We acknowledge DHS’s concern that its working relationship with the chemical industry might be constrained by

---

too close association with EPA, which regulates the industry. However, we do not believe that a DHS-EPA partnership to study the potential security benefits of using safer chemicals and technologies would necessarily bring the department into conflict with the industry, if the appropriate informational safeguards and assurances are built into the process. Through additional study, DHS—in conjunction with EPA—can help to determine the appropriate role of inherently safer technologies in government and industry efforts to bolster chemical facility security. Through such an effort, DHS and EPA could also identify alternative ways to reduce both security and environmental and health risks and share these practices with private industry.

DHS also provided a number of technical comments and clarifications, which we have incorporated into the report as appropriate. Appendix III contains the full text of DHS's comments in a letter dated December 8, 2005.

---

As arranged with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this report. At that time, we will send copies to other interested congressional committees and to the Secretary of the Department of Homeland Security and the Administrator of the Environmental Protection Agency. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.



---

If you or your staff have any questions on this report, please contact me at (202) 512-3841 or at [stephensonj@gao.gov](mailto:stephensonj@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other GAO staff who contributed to this report are listed in appendix IV.

A handwritten signature in black ink that reads "John B. Stephenson". The signature is written in a cursive style with a long horizontal flourish at the end.

John B. Stephenson  
Director, Natural Resources  
and Environment

---

# Objectives, Scope, and Methodology

---

Our objectives were to describe (1) the Department of Homeland Security's (DHS) actions to develop an overall strategy for protecting the chemical industry; (2) DHS's efforts to identify high-risk chemical facilities, assess their vulnerabilities, ensure that facilities are addressing security, and coordinate with the Environmental Protection Agency (EPA) in these efforts; (3) chemical industry security initiatives and challenges; and (4) DHS's existing authorities, and whether additional legislative authority is needed to ensure that chemical facilities take action to address vulnerabilities. To discuss DHS's actions to develop an overall strategy for protecting the chemical industry, we reviewed DHS's February 2005 Interim National Infrastructure Protection Plan, its April 2004 guidance to sector-specific agencies on drafting sector plans, and a July 2004 draft of its Chemical Sector-Specific Plan.

To discuss the actions DHS has taken to identify high-risk chemical facilities, assess their vulnerabilities, ensure that facilities are addressing security, and coordinate with EPA, we interviewed officials from DHS's Information Analysis and Infrastructure Protection Directorate and EPA's Office of Emergency Management and gathered and reviewed available documents and reports from both agencies. Specifically, in addition to the documents previously mentioned, we reviewed DHS reports on chemical facilities' and chemical storage facilities' characteristics and their common vulnerabilities and potential indicators of terrorist activity, one-page summaries of DHS programs provided by department officials, and other available reports and information on DHS efforts. We also attended two industry-sponsored conferences, which included detailed presentations from DHS officials on the department's chemical security efforts. In addition, we interviewed contractors for DHS's Risk Analysis Management for Critical Asset Protection (RAMCAP) initiative; representatives from the American Society of Mechanical Engineers; and the subcontractor developing chemical sector RAMCAP tools, the AcuTech Consulting Group. In addition, we reviewed EPA Risk Management Plan (RMP) data and obtained EPA officials' views on DHS's analysis of these data to identify high-risk chemical facilities. We also discussed current interagency coordination and opportunities for additional coordination between DHS and EPA with officials from both agencies.

To discuss chemical industry voluntary initiatives and challenges, we met with representatives of all 16 associations participating on the Chemical Sector Coordinating Council.<sup>1</sup> Using structured interview questions, we gathered representatives' views on threats, DHS's chemical security efforts, and industry security initiatives. We also reviewed documents from industry associations, such as vulnerability assessment tools, descriptions of voluntary security programs, security guidelines, and best practices. We used this information to assess the various initiatives undertaken by associations and their members. To obtain a broad range of industry views, we also talked to representatives of 20 chemical companies belonging to 13 of the 16 associations on the Chemical Sector Coordinating Council. Officials of some of these companies were present at our meetings with associations, while others were contacted by industry associations and agreed to speak with us separately. Three associations—the Adhesive and Sealant Council, the International Institute of Ammonia Refrigeration, and the National Paint and Coatings Association—were not able to identify a member company willing to speak with us. We also gathered information from both industry associations and chemical company officials about challenges companies face in improving security. To avoid unintentionally disclosing any security-related information, we are not disclosing the names or other identifying information relating to the individual chemical companies we contacted. The comments from industry officials discussed in this report are illustrative, are not statistically representative of the chemical sector, and should not be considered to represent the views of the chemical sector as a whole.

To discuss DHS's existing authorities and whether additional legislative authority is needed to ensure that chemical facilities take action to address vulnerabilities, we analyzed DHS's current authorities and gathered a range of views on the need for additional authority. Specifically, we analyzed DHS's current authorities under the Homeland Security Act of 2002, the Patriot Act, and other laws. DHS officials would not comment directly to us on the department's need for additional authority because the executive

---

<sup>1</sup>As of November 2005, Chemical Sector Coordinating Council members included the Adhesive and Sealant Council; the American Chemistry Council; the American Forest and Paper Association; the Chemical Producers and Distributors Association; the Chlorine Chemistry Council; the Chlorine Institute; the Compressed Gas Association; CropLife America; the Fertilizer Institute; the Institute of Makers of Explosives; the International Institute of Ammonia Refrigeration; the National Association of Chemical Distributors; the National Paint and Coatings Association; the National Petrochemical and Refiners Association; the Society of the Plastics Industry, Inc.; and the Synthetic Organic Chemical Manufacturers Association.

branch has not yet established a unified position on this issue. However, we were able to obtain DHS's views on legislation by reviewing DHS statements and comments at hearings on chemical facility security in July 2005. We also gathered views on the need for legislation and the content and structure of legislation during interviews with EPA, industry associations, chemical companies, state homeland security officials in New Jersey and Texas, and other organizations with chemical industry expertise. These organizations included the American Institute of Chemical Engineers' Center for Chemical Process Safety; Sandia National Laboratories; the U.S. Chemical Safety and Hazard Investigation Board; the American Society of Mechanical Engineers; the University of Pennsylvania Wharton School's Risk Management and Decision Processes Center; Texas A&M University's Mary K. O'Connor Process Safety Center and National Emergency Response and Rescue Training Center; OMB Watch; the Working Group on Community Right-to-Know; U.S. Public Interest Research Group; and the Paper, Allied-Industrial, Chemical, and Energy Workers International Union. We also asked representatives of these organizations and industry officials about challenges the federal government faces in securing the nation's chemical facilities from a terrorist attack. In addition, we reviewed the testimony of industry officials and other experts on legislation at hearings before the Senate Homeland Security and Governmental Affairs Committee and the House Homeland Security Committee, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity, in April, June, and July 2005.

We limited our review of security issues to stationary chemical facilities and did not address security concerns surrounding the transportation of hazardous chemicals. We conducted our work from December 2004 through December 2005 in accordance with generally accepted government auditing standards.

---

# Summary of the Chemical Industry's Voluntary Security Initiatives

---

Sixteen chemical industry associations participate in the Chemical Sector Coordinating Council and have initiated a variety of security efforts. These efforts range from developing security guidance and best practices to establishing security requirements that member facilities must follow to remain eligible for association membership.

The following is a brief description of these 16 associations and a summary of security efforts under way at the facilities owned and/or operated by their member companies.

---

## American Chemistry Council

The American Chemistry Council (ACC) has 135 members that represent the leading companies in the U.S. chemical manufacturing sector. According to ACC, its members are responsible for nearly 90 percent of basic industrial chemical production. ACC's member companies operate about 2,000 facilities, approximately 1,000 of which are RMP facilities. Approximately 270 of ACC's member facilities are also subject to the Maritime Transportation Security Act of 2002 (MTSA).

ACC adopted a Responsible Care® Security Code that outlines 13 management practices that company security management systems must include. These practices require companies to perform security vulnerability assessments of their facilities, develop and implement plans to mitigate the vulnerabilities, and obtain third-party verification that the planned physical security enhancements were completed. ACC members assigned its facilities into "tiers" on the basis of the potential impact a chemical release at a facility would have on surrounding communities, and these facilities must follow milestone dates for completing security requirements that are based on tier level. ACC reported that as of May 2004, all of its 2,000 facilities have completed security vulnerability assessments at their sites using the Sandia National Laboratories vulnerability assessment methodology, the Center for Chemical Process Safety methodology, or an equivalent methodology approved by the center.

The Responsible Care® Security Code also requires that companies apply security management practices to facility cyber assets and the chemical industry distribution chain, which covers the complete "value chain" for chemicals, from suppliers to customers, including transportation. Member companies must perform vulnerability assessments of their cyber assets and distribution value chain and implement plans to mitigate these vulnerabilities. ACC asked that a company executive from each member provide a signed statement declaring that the company had management

---

systems in place for the entire security code by June 30, 2005. As of October 3, 2005, 95 percent of member companies have signed this statement. ACC officials told us that a number of companies have left ACC over the last few years because of the cost of complying with Responsible Care® requirements. Recognizing the degree of rigor associated with the Responsible Care® Security Code, the United States Coast Guard recognized the code as an alternative security program for purposes of fulfilling facility security requirements under MTSA.

---

**American Forest & Paper Association**

The American Forest & Paper Association has 116 members, including companies that manufacture pulp, paper, paperboard, wood, or related products in the United States. According to the association, its member companies operate over 1,000 facilities, of which 80 to 90 are RMP facilities. The association has established no specific security requirements for its members, but has provided them with guidance on facility site security principles and distributed pamphlets on common steps for protecting forest products industry infrastructure.

---

**Chemical Producers and Distributors Association**

The Chemical Producers and Distributors Association represents 86 member companies engaged in (1) the manufacture, formulation, distribution, and sale of crop protection chemicals, fertilizers, feed, fiber crops, and ingredients used in food; (2) the care and maintenance of lawns, gardens, and turf; and (3) various forestry and vegetation management markets. The association has established no specific security requirements for its members, but shares information about security issues with members at meetings and conferences.

---

**Chlorine Chemistry Council**

The Chlorine Chemistry Council is a business council of ACC representing the manufacturers and users of chlorine and chlorine-related products. The council has seven voting members, who must be members of ACC and comply with ACC's Responsible Care® security requirements. Most facilities of voting member companies are also RMP facilities. The council also has nonvoting members who are not ACC members. Some of these members voluntarily follow the general approach of Responsible Care®.

---

**Compressed Gas Association**

The Compressed Gas Association (CGA) has 138 member companies that represent manufacturers, distributors, suppliers, and transporters of gases

and cryogenic liquids (i.e., liquefied gases kept in a liquid state at extremely low temperatures). The association's members have gases, such as oxygen, nitrogen, argon, and helium, that are used in most industries, including food and metal processing, semiconductor manufacturing, healthcare, and chemical production. According to CGA, member companies include approximately 15 to 20 industrial gas manufacturing companies. CGA does not collect information on the number of facilities member companies have that must meet RMP requirements. Some member companies that make gas products used in foods must comply with aspects of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 to protect the nation's food, according to CGA.

CGA has established no specific security requirements for members, but has developed and distributed guidance to the compressed gas industry on assessing security risks and identifying and implementing preventive security measures. Guidelines address site security, transportation security, and steps facilities should take to "qualify" customers, (i.e., ensure that they are purchasing products for the appropriate uses). CGA relied heavily on site security guidelines developed by ACC, the Chlorine Institute, and the Synthetic Organic Chemical Manufacturers Association in 2001 and on information from the Center for Chemical Process Safety in developing these guidelines.

---

## CropLife America

CropLife America represents the developers, manufacturers, formulators, and distributors of chemicals for agriculture and pest management in the United States. CropLife America member companies produce, sell, and distribute virtually all of the crop protection and biotechnology products used by American farmers. CropLife America's membership includes 18 pesticides manufacturing companies with about 30 facilities and 5 integrated distribution companies with 1,100 of the nation's 5,500 bulk pesticide retail agricultural facilities, which typically store both fertilizer chemicals and pesticides. All of the manufacturing facilities are subject to RMP. Most of the retail facilities also are subject to RMP because they house ammonia. CropLife America also has about 10 member facilities that formulate pesticides. CropLife America also participates in the Food and Agriculture Sector Coordinating Council.

Six of CropLife America's basic research and manufacturing members are ACC members and their facilities adhere to the Responsible Care® Security Code. In addition, working with the Agricultural Retailers Association, CropLife America created a not-for-profit organization called

the American Agronomic Stewardship Alliance to develop a stewardship inspection and accreditation program for its agricultural retail and distribution facilities that includes some security steps. The alliance requires facilities to develop security plans and undergo inspection by third-party vendors that includes checking to see that security plans were prepared. However, the inspectors do not look at whether the security plan has been implemented. As of April 2005, third parties had completed about 2,000 inspections and 98 percent of inspected facilities had a security plan on file. CropLife America also published security guidelines shortly after the events of September 11, 2001, and has distributed these guidelines extensively.

---

**Institute of Makers of Explosives**

The 40 member companies of the Institute of Makers of Explosives (IME) include explosives manufacturers and distributors, and companies that are contracted by mining companies to conduct explosions. According to IME, about 30 of IME's member companies manufacture or distribute explosives at about 300 facilities. Six of these companies operate 23 RMP facilities.

IME member companies are subject to a number of safety and security requirements regulated by the Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives. IME has no specific security requirements for its members, but has provided recommended security guidelines to its members that include conducting a vulnerability assessment but does not audit members for compliance. IME also has work under way on a risk assessment modeling tool for accident risk planning that will include a terrorist threat scenario. The model is based on Department of Energy work and is intended for manufacturers and drill blast companies.

---

**International Institute of Ammonia Refrigeration**

The International Institute of Ammonia Refrigeration is an international association serving companies that use ammonia refrigeration technology, including end users such as food refrigeration companies, contractors, engineers, equipment manufacturers, and others in the industry. While the institute was unable to provide the number of RMP facilities in its membership, about 2,000 RMP facilities use ammonia refrigeration. According to the institute, these ammonia refrigeration facilities include approximately 600 refrigerated warehouses and storage facilities, such as regional food distribution centers, and about 400 facilities that house meat from slaughterhouses. Almost all of the food facilities belonging to the institute are covered by the Bioterrorism Act. The institute also



participates in DHS's Agriculture Sector Coordinating Council. The institute has established no specific security requirements for its members, but shares information about security issues with its members at annual meetings.

---

**National Association of  
Chemical Distributors**

Member companies of the National Association of Chemical Distributors (NACD) package, distribute, and blend chemicals. Its members typically work with chemicals that do not react in unstable ways and store large quantities of chemicals in warehouses. NACD represents 253 chemical distribution companies that own, lease, or manage approximately 1,380 facilities in the United States and Canada. NACD estimates that at least 350 member facilities are RMP facilities.

In 1991, NACD developed an environment, health, safety, and security management protocol called the Responsible Distribution Process. Adherence to this process is a condition of NACD membership. Since January 1999, NACD members have been required to have their successful implementation of all required membership practices verified by third parties once every 3 years. NACD contracted with an internal auditing company to be the third-party reviewer for its members. The first 3-year cycle of Responsible Distribution Process verification ended in December 2001. In April 2002, NACD added security measures to the process, which require its members to develop security programs, scrutinize security measures taken by for-hire motor carriers, ensure that customers are purchasing chemicals for the appropriate use (as prescribed by government regulations), and verify implementation of security measures by an independent firm designated by NACD. The second 3-year cycle for process verification began in January 2003 and ended in December 2005. Beginning in January 2006, NACD's Responsible Distribution Process includes a requirement that members conduct security vulnerability assessments. NACD developed its own vulnerability assessment methodology, and members will be expected to have completed their assessment by June 2006. NACD has terminated the membership of 20 companies that failed to comply with the Responsible Distribution Process requirements and to complete and pass the verification step.

---

**National Paint and Coatings  
Association**

The National Paint and Coatings Association (NPCA) represents manufacturers and suppliers of paints and coatings, including lacquers, stains, varnishes, and concrete. NPCA has over 350 associate and full-member companies, representing an estimated 700 paint manufacturing

facilities that range from mom-and-pop stores to chain stores. Approximately 50 of these facilities are RMP facilities. NPCA worked with its members to develop Coatings Care, a safety and environmental management system that includes security steps such as analyzing threats, vulnerabilities, and consequences and the implementation of security measures. Coatings Care also includes a vulnerability assessment methodology developed by a member company specifically for paint and coatings facilities that companies may elect to use, as well as examples of security checklists and best practices. Member companies have 1 year from the time they become NPCA members to agree to follow the Coatings Care principles. However, NPCA does not require that members take steps to verify their compliance with Coatings Care security requirements.

---

**National Petrochemical and Refiners Association**

The National Petrochemical and Refiners Association (NPRRA) has about 450 member companies that include refiners and petrochemical manufacturers, suppliers, and vendors. Almost all U.S. refiners are NPRRA members, which represent about 98 percent of the total refining capacity in the United States. Petrochemical manufacturing facilities use processes similar to those used in refineries and are often colocated at refineries. According to NPRRA, a majority of the almost 150 refineries and 200 petrochemical manufacturing facilities in the United States are subject to MTSA. Because refineries are currently considered to be part of the energy critical infrastructure sector, NPRRA also participates in the Oil and Natural Gas Sector Homeland Security Coordinating Council, which meets regularly with a sector government coordinating council that includes DHS and the Department of Energy. NPRRA has established no specific security requirements for its members, but it holds security conferences and workshops for its members that address security issues. In addition, NPRRA and the American Petroleum Institute developed a vulnerability assessment methodology for petrochemical manufacturing and refining facilities that was issued in 2003 and updated in 2004. The Center for Chemical Process Safety has approved the methodology. DHS formally acknowledged that the methodology can be used to satisfy MTSA requirements.

---

**Synthetic Organic Chemical Manufacturers Association**

The Synthetic Organic Chemical Manufacturers Association (SOCMA) includes 160 member companies that operate about 300 small- to medium-sized specialty chemical manufacturing facilities in the United States, or "batch" facilities, that produce a diverse number of chemicals. Specialty chemicals are formulated to meet the detailed specifications of various end users, and usually have unique purposes, such as making nylon fibers

stronger or serving as the active ingredient in medicine. In December 2002, SOCMA adopted ACC's Responsible Care® Security Code. SOCMA also developed a vulnerability assessment methodology reflecting the variable risks at smaller facilities. According to SOCMA officials, as of September 2005, all of its member companies had reported completing vulnerability assessments and 98 percent of these companies reported that they had implemented security enhancements and obtained third-party verification. However, beginning in October 2005, SOCMA no longer required its members to adhere to Responsible Care® because it has developed its own environmental, health, safety, and security performance program. SOCMA's new program, called ChemStewards<sup>SM</sup>, will still require members to conduct vulnerability assessments and implement enhancements for physical security but will not include specific security requirements for cyber assets and facilities' distribution chain, which covers the complete value chain for chemicals, from suppliers to customers, including transportation. According to SOCMA, they have taken this step because cybersecurity issues are far less significant for small companies, most of whom do not use process control systems that can be disrupted via cyber attack. Members will have to obtain third-party verification of security improvements if a facility is an RMP facility.

---

### The Adhesive and Sealant Council

The Adhesive and Sealant Council (ASC) represents adhesive and sealant manufacturers and supplier companies. The council has about 126 member companies with approximately 250 facilities. According to ASC, most of these facilities are RMP facilities. About 75 or 80 member companies are raw materials suppliers, some of which also belong to ACC and, therefore, comply with Responsible Care®. About 55 member companies are adhesives or sealant manufacturers, some of which also belong to NPCA. ASC has no specific security requirements for members.

---

### The Chlorine Institute

The Chlorine Institute represents approximately 220 member companies that produce, distribute, and use chlorine, sodium, and potassium hydroxides and sodium hypochlorite, and that distribute and use hydrogen chloride. The institute's North American producer members account for 98 percent of the total chlorine production capacity of the United States and Canada; its packager member companies represent 100 percent of the total U.S. market. Most of the facilities of the institute's member companies are RMP facilities. A few of the institute's members are large water treatment facilities that are covered by the Bioterrorism Act, and many of their members also have facilities covered by MTSA, according to the institute.

The Chlorine Institute encourages, but does not require, its members to conduct vulnerability assessments and develop security plans. Member companies that are also ACC members conduct vulnerability assessments and develop security plans in accordance with the Responsible Care® Security Code. The institute has developed a seven-step process that smaller chlorine manufacturing and distribution companies can use to assess their vulnerabilities. In addition, the institute requires executives of all member companies to sign an agreement stating that they will meet nine safety and security requirements, including complying with Responsible Care® or another industry security program. Companies whose executives do not sign the agreement are not eligible for institute membership. The institute does not require that companies take steps to verify that vulnerability assessments and security plans are completed and security measures are implemented.

---

### The Fertilizer Institute

The Fertilizer Institute (TFI) represents companies that make, sell, and transport fertilizer products. Its approximately 190 member companies operate retail spaces, warehouses, terminal, and production facilities. Approximately 20 companies in the United States manufacture fertilizer. TFI has established no specific security requirements for its members. In 2002, however, TFI developed a Security Code of Management Practices that it recommends, but does not require, that members follow. The security code involves screening facilities into priority tiers that are based on potential security hazards and, following a timeline on the basis of tier level, conducting a vulnerability assessment using a methodology developed by the Center for Chemical Process Safety, SOCMA, or other equivalent methods. Also in 2002, a working group comprising members of TFI, CropLife America, and the Agriculture Retailers Association, developed a Web-based vulnerability assessment tool for agribusiness retail facilities. The Center for Chemical Process Safety approved the tool as meeting its criteria for security vulnerability assessments. According to TFI, approximately 2,000 of its member retail facilities have used the tool to date.

---

### The Society of the Plastics Industry, Inc.

The Society of the Plastics Industry, Inc., represents the entire plastics industry, including processors, machinery and equipment manufacturers, and raw materials suppliers. The society has about 1,100 member companies—about half of these companies supply machinery (auxiliary components, dryers, and heavy equipment, among others); about 250 to 300 companies process and recycle plastics; less than 100 companies make

---

**Appendix II**  
**Summary of the Chemical Industry's**  
**Voluntary Security Initiatives**

---

resins; and the remaining companies make molds. The bulk of the society's member companies do not handle large quantities of hazardous chemicals. The society has established no specific security requirements for its members. Some of the society's members are also members of ACC or the Synthetic Organic Chemical Manufacturers Association and, therefore, comply with these associations' security programs.

# Comments from the Department of Homeland Security

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

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

December 8, 2005

Mr. John Stephenson  
Director Natural Resources and Environment  
U.S. Government Accountability Office  
Washington, D. C. 20548

Dear Mr. Stephenson:

RE: Draft Report GAO-05-150 DHS is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority is Needed (GAO Job Code 360538)

Thank you for the opportunity to review the draft report. In addition to responses to the two recommendations contained in the report, we are providing general comments that are more than technical in nature and are responsive to content in the text of the report.

**Recommendation:** The Congress considers giving the Department of Homeland Security (DHS) authority to require the chemical industry to address plant security.

**Response:** Concur in Part. DHS agrees the Congress should consider giving DHS authority to require the chemical industry to address plant security in the interest of enhancing security at these facilities.

**Recommendation:** DHS complete the chemical sector-specific plan in a timely manner and work with the Environmental Protection Agency (EPA) to study the security benefits to chemical plants of using safer technologies.

**Response:** Non-concur. DHS does not concur with the recommendation as stated. The Office of Infrastructure Protection (IP) agrees that completing and implementing the sector-specific plan is a priority and is making significant progress toward developing a final plan. However, IP recommends GAO strike the mention of DHS working with EPA to study safer technologies. DHS believes that safer technologies would not generally result in more secure chemical facilities. The use of inherently safer technologies tends to shift risks rather than eliminate risks, often with unintended consequences. It is also unclear what EPA's role would be in this context, or how DHS interaction with EPA in this regard might be perceived among our private sector partners.

[www.dhs.gov](http://www.dhs.gov)

See comment 1.

*General Comments*

**General Item: 1**

**Page: 3, 15**

Issue summary: DHS is developing a national strategy for protecting the chemical sector, which department officials expect to complete in 2006. This strategy- to be included in a Chemical Sector-Specific Plan- is intended to outline a framework for reducing the overall vulnerability of the chemical sector in partnership with industry, state and local authorities, according to DHS officials... As a part of the National Infrastructure Protection Plan (NIPP), DHS is developing a national strategy for protecting the chemical sector that will establish a framework for reducing the overall vulnerability of the sector in partnership with the industry and state and local authorities.

**DHS/IP Statement:** The National Strategy being developed for the Chemical Sector is separate but complimentary to the Chemical Sector Specific Plan. The National Strategy for Securing the Chemical Sector, which was requested by Congress in the committee report for the FY06 Homeland Security appropriations bill, is a high-level strategic document being prepared solely by DHS. The Chemical Sector Specific Plan (SSP), which will be an appendix to the National Infrastructure Protection Plan (NIPP), is a strategic & operational document being prepared by DHS in conjunction with other Federal agencies, State and local governments, and the private sector. The Chemical SSP, like SSPs for all 17 critical infrastructure and key resource sectors, cannot be completed until the NIPP Base Plan is completed, and is scheduled to be completed within six months of the signing out of the NIPP Base Plan.

See comment 2.

**General Item: 2**

**Page: 4**

Issue: "Conducting this analysis will require that chemical facility owners and operators voluntarily assess their own risks and provide DHS with this information."

**DHS/IP Statement:** DHS would like owners and operators to assess and provide information on their vulnerabilities and potential consequences of an attack. An accurate assessment of risk requires specific threat information, which may not be available in all cases.

See comment 3.

**General Item: 3**

**Page: 19, FN 12**

Issue: EPA has expressed concern about DHS' analysis of the Risk Management Plan (RMP) database. According to EPA officials, the results of DHS analysis appear to indicate that the data may have been manipulated incorrectly. For example, EPA does not agree that the database contains 3,000 facilities that are no longer in business or no longer RMP facilities. EPA officials offered to assist DHS with implementation of the RMP database.

**Appendix III  
Comments from the Department of Homeland  
Security**

See comment 4.

**DHS/IP Statement:** Please note in the GAO Report that DHS is open to working with EPA to clarify the Department's methodology for interpreting the RMP database as it relates to risk.

**General Item: 4**

Page: 21

Issue: According to DHS, 272 of these facilities could potentially affect more than 50,000 people. These 272 facilities include chemical manufacturing plants as well as refineries, wastewater treatment facilities, and other types of chemical facilities.

**DHS/IP Statement:** This states that the 272 facilities include refineries and wastewater treatment facilities. However, in regard to refineries, the list mainly includes petrochemical companies. In addition, it should be noted that wastewater treatment facilities were not intended to be incorporated in the list of top facilities.

See comment 5.

**General Item: 5**

Page: 22

Issue: According to DHS officials, DHS plans to ask 20,000 chemical facility owners/operators to complete the Risk Analysis Management for Critical Asset Protection (RAMCAP) top screen. DHS will work with industry associations to distribute the RAMCAP screening tool to chemical facilities. DHS officials said that they expect that less than 1,000 chemical facility owners/operators will be asked to complete the vulnerability assessment.

**DHS/IP Statement:** This states that DHS plans to ask 20K facilities to do the Top Screen and 1K to do the Site Vulnerability Assessment (SVA). DHS recommends that GAO strike the mention of 20,000 facilities as this number is subject to change.

***IP Proposed Replacement Language:*** According to DHS officials, DHS will work with industry associations to distribute the RAMCAP screening tool to the highest consequence chemical facilities. DHS officials expect that between 5-10 percent of those chemical facility owners/operators will be asked to complete the self vulnerability assessment.

See comment 6.

**General Item: 6**

Page: 23

Issue: According to industry officials, however, the companies who pre-tested the security vulnerability assessment found the exercise valuable and difficult to complete.

**DHS/IP Statement:** The GAO Report says companies pre-tested the SVA, but they actually tested the Top Screen, not the SVA.

See comment 7.

**General Item: 7**

Page: 27

Issue: DHS is also planning a series of Comprehensive Reviews in areas with large number of chemical facilities, focusing on facilities' security as well as emergency



---

**Appendix III**  
**Comments from the Department of Homeland**  
**Security**

---

response capabilities in the local area. A team of federal officials from multiple agencies along with state and local officials will plan and conduct the work... DHS hopes to complete 5 visits to clusters of facilities during 2006.

**DHS/IP Statement:** DHS expects to visit 6 Comprehensive Review (CR) clusters in 2006, not 2005. Also, the description says that state and local officials will plan and conduct the work. Actually, the planning and conduct of the actual work is all going to be done by the various federal agencies involved in the CR effort in coordination with State and local officials

*IP Suggested Language: The Comprehensive Review is a DHS-led cooperative government and private sector analysis of Critical Infrastructure/ Key Resource (CI/KR) that will enhance public safety by helping the nation prevent and prepare for a potential terrorist attack, identify and reduce the possible consequences of such an attack, and enhance the integrated prevention and response capabilities of the owner/operator, local law enforcement, and emergency response organizations. The results will be used to enhance the nation's security posture by implementing short-term protective measures and making longer-term risk-based investments in training, processes, procedures, and resources for the community. The Comprehensive Review process also provides an opportunity for all affected stakeholders to identify and implement best practices for readiness and preparedness for any catastrophic event affecting critical infrastructure.*

See comment 8.

**General Item: 8**

Page: 48

Issue: Set of principles proposed for chemical security legislation

- Require a common set of standards and practices to level the playing field across the chemical sector;
- Implement core security measures consistently and fairly, based on risk;
- Give DHS the authority to decide which facilities will be subjected to any new rules, based on the risk of a terrorist attack;
- Give DHS the flexibility to address security issues for individuals facilities on a case-specific basis;
- Provide DHS the authority, with sufficient flexibility, to address specific threats to high-risk facilities, or under extraordinary circumstances;
- Recognize and build upon public- and private-sector work and investment to date, and avoid penalizing companies already operating under existing Federal security authorities (for example MTSA), where appropriate;
- Do not halt or deter ongoing capital investment by companies that are taking responsible security measures currently;
- Balance the need for appropriate security measures with the ability to effectively and efficiently maintain business operations;
- Institute market-based incentives to the highest degree possible to secure the chemical sector;

4

Appendix III  
Comments from the Department of Homeland  
Security

- Include an objective verification and validation process for ensuring that adequate security measures implanted, and allow the Security of DHS to issue civil penalties for non-compliance; and
- Protect confidential, proprietary, and business sensitive information

**DHS/IP Statement:** This list differs from the current list of principles for proposed chemical legislation. The following text represents the current list of principles, which were outlined during testimony that DHS believes should be incorporated into any potential legislation:

*“First, we must recognize that not all facilities present the same level of risk, and that the most scrutiny should be focused on those that, if attacked, could endanger the greatest number of lives, have the greatest economic impact or present other very significant risks. Second, facility security should be based on reasonable, clear, and equitable performance standards. The Department should develop enforceable performance standards based on the types and severity of potential risks posed by terrorists, and facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those risks. Third, we should recognize the progress many responsible companies have made to date.”*

**General Item: 9**

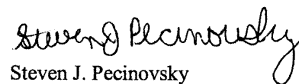
Page: 52

Issue: Furthermore, DHS’ July 2004 draft Chemical Sector-Specific Plan states that inherently safer chemistry and engineering practices can prevent or delay a terrorist incident, noting that it is important to make sure that facility owners/operators consider alternative ways to reduce risk such as inherently safer design, implementing just-in-time manufacturing , or replacing high-risk chemicals with safer alternatives.

**DHS/IP Statement:** Inherently Safer Technology (IST) does not “prevent or deny” incidents. The use of inherently safer technologies tends to shift risks rather than eliminate risks, often with unintended consequences. It is also unclear what EPA’s role would be in this context.

We thank you again for the opportunity to review the report and provide comments.

Sincerely,



Steven J. Pecinovsky  
Director  
Departmental GAO/OIG Liaison Office

See comment 9.

---

The following are GAO's comments on the Department of Homeland Security's letter dated December 8, 2005.

---

## GAO Comments

1. We revised the report to include a description of the National Strategy for Securing the Chemical Sector.
2. We revised the report to include the language suggested by DHS.
3. We revised the report to include DHS's statement that it is open to working with EPA on interpreting the RMP database. In addition, we encourage DHS to share its analysis of the database with EPA to ensure that all high-risk facilities are identified.
4. We revised the report to state that the 272 facilities that could potentially affect more than 50,000 people included some refineries located with petrochemical companies. We also added DHS's comment that it did not intend to incorporate wastewater treatment facilities into the list of top facilities.
5. We revised the report to indicate that DHS is uncertain how many facilities it will ask to complete the RAMCAP top screen.
6. Contrary to DHS's statement, industry officials told us that the companies that pretested the security vulnerability assessments—not the top screen, as DHS indicates—found the exercise valuable, but difficult to complete. As of early November 2005, four chemical companies had tested the security vulnerability assessment at one of its facilities.
7. We revised the report to state that DHS expects to conduct six Comprehensive Reviews, and that they will coordinate these reviews with state and local officials.
8. As DHS suggested, we deleted the list of principles for proposed chemical security legislation that DHS officials provided us in October 2005 and substituted the language suggested by DHS, which was, in part, already included in the draft report.
9. As we state in our response to DHS's views on our recommendation, we continue to believe that the use of safer technologies may potentially reduce both security and environmental and health risks at some

---

chemical facilities. We retained the draft report's existing discussion of the issue, including DHS's and the industry's views, but added DHS's specific statement from its comment letter that "the use of inherently safer technologies tends to shift risks rather than eliminate risks, often with unintended consequences." We also included information from DHS's draft Chemical Sector-Specific Plan, which states that inherently safer chemistry and engineering practices can prevent or delay a terrorist incident, and that it is important to make sure that facility owners/operators consider alternate ways to reduce risk, such as inherently safer design, implementing just-in-time manufacturing, or replacing high-risk chemicals with safer alternatives.

# GAO Contact and Staff Acknowledgments

---

---

**GAO Contact**

John B. Stephenson (202) 512-3841

---

**Staff  
Acknowledgments**

In addition, Vincent P. Price, Assistant Director; Leigh White; Joanna Owusu; and Jill Edelson made key contributions to this report. Important contributions were also made by John W. Delicath and Amy Webbink.

---

## GAO's Mission

The Government Accountability 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 GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to Updates."

---

## 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. Government Accountability 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](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Gloria Jarmon, Managing Director, [JarmonG@gao.gov](mailto:JarmonG@gao.gov) (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, D.C. 20548

---

## Public Affairs

Paul Anderson, Managing Director, [AndersonP1@gao.gov](mailto:AndersonP1@gao.gov) (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548