

**GAO**

Report to the Honorable Robert C. Byrd, Ranking Member, Subcommittee on Homeland Security, Committee on Appropriations, U.S. Senate

---

March 2005

# PROTECTION OF CHEMICAL AND WATER INFRASTRUCTURE

## Federal Requirements, Actions of Selected Facilities, and Remaining Challenges





Highlights of [GAO-05-327](#), a report to the Honorable Robert C. Byrd, Ranking Member, Subcommittee on Homeland Security, Committee on Appropriations, U.S. Senate

## Why GAO Did This Study

The National Strategy for Homeland Security grouped critical infrastructure into 13 sectors which include assets that if attacked by terrorists could have a debilitating impact on the nation. Two of these 13 sectors are the chemical and water sectors. The total number of chemical sector facilities is not clear. DHS estimates that there are 4,000 chemical manufacturing facilities that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment. There are approximately 53,000 community water systems and more than 2,900 maritime facilities that are required to comply with security regulations under the Maritime Transportation Security Act (MTSA). This report provides information about what federal requirements exist for the chemical and water sectors to secure their facilities, what federal efforts were taken by the lead agencies for these sectors to facilitate sectors' actions, what actions selected facilities within these sectors have taken and whether they reflect a risk management approach, what obstacles they say they faced in implementing enhancements, and what are the Coast Guard's results from its inspection of regulated maritime facilities' security enhancements.

## What GAO Recommends

Because GAO has previously made recommendations on the key issues discussed in this report, we are not making any new recommendations.

[www.gao.gov/cgi-bin/getrpt?GAO-05-327](http://www.gao.gov/cgi-bin/getrpt?GAO-05-327).

To view the full product, including the scope and methodology, click on the link above. For more information, contact William O. Jenkins, Jr., (202) 512-8777, or [jenkinswo@gao.gov](mailto:jenkinswo@gao.gov).

# PROTECTION OF CHEMICAL AND WATER INFRASTRUCTURE

## Federal Requirements, Actions of Selected Facilities, and Remaining Challenges

### What GAO Found

Few federal requirements address the security of the chemical and water sectors. However, the Department of Homeland Security (DHS) and the Environmental Protection Agency (EPA) have taken actions to assist the chemical and water sectors to implement security enhancements including providing financial assistance in the form of grants, threat information and guidance, training and exercises, and infrastructure protection initiatives, as well as setting security requirements for some facilities and reviewing actions by maritime facilities to determine compliance with MTSA. Except for facilities covered by MTSA, the chemical sector's security efforts are not regulated. The water sector is regulated by the Bioterrorism Act of 2002, which, among other things, requires community water systems to perform vulnerability analyses of their facilities.

Chemical facilities and community water systems reported making security improvements separate from federal requirements. The chemical industry's two principal trade associations require their members to follow a security code that includes elements of a risk management framework such as completing vulnerability assessments and taking actions based on those assessments. Officials at all 10 chemical facilities GAO visited reported making significant progress in implementing the trade associations' security code. However, the proportion of total chemical facilities covered by the code is uncertain. The 8 water systems GAO visited reported completing their required vulnerability assessments, which is one element of a risk management framework. Although community water systems are not required to take any risk reduction measures under the Bioterrorism Act, these 8 water systems reported implementing a number of enhancements, such as increasing access controls.

Officials representing 8 of the 10 chemical facilities and 8 community water systems GAO visited reported encountering obstacles in making security enhancements and maintaining a level of security consistent with their needs. Officials at 3 chemical facilities reported experiencing difficulties, such as delays, in obtaining permits or other approvals needed from federal authorities to install fences to better protect the perimeter of their facilities. Officials at 6 of the community water systems GAO visited reported economic constraints, such as balancing the need for rate increases to fund security enhancements with efforts to keep rates low.

MTSA's security requirements cover more than 2,900 maritime facilities, including chemical facilities. The Coast Guard found that 97 percent of these facilities complied with MTSA and its implementing regulations. The Coast Guard took 312 enforcement actions against 98 facility owners and operators and imposed operational controls on 29 facilities across the more than 2,900 MTSA-regulated facilities. DHS and EPA generally concurred with the contents of the report.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	4
	Background	8
	Few Federal Security Requirements Exist for the Chemical and Water Sectors, but Other Federal Actions Have Facilitated these Sectors' Efforts to Enhance Security	12
	Chemical Facilities and Water Systems Reported Taking Actions to Address Security Vulnerabilities but Said They Faced Obstacles in Implementing Security Measures	17
	The Chemical and Water Sectors Have Incorporated Some Elements of a Risk Management Framework to Address Their Security Vulnerabilities	24
	Officials at Chemical Facilities and Water Systems We Visited Agreed in Part about What the Federal Government's Role Should Be	29
	The U.S. Coast Guard Completed Its Compliance Inspections and Plans to Review the Effectiveness of the Process	30
	Agency Comments	31
<b>Appendix I</b>	<b>Scope and Methodology</b>	<b>34</b>
<b>Appendix II</b>	<b>Number of Community Water Systems</b>	<b>38</b>
<b>Appendix III</b>	<b>Chemical Industry Trade Associations' Implementation of the Responsible Care® Security Code</b>	<b>39</b>
<b>Appendix IV</b>	<b>Enforcement Actions Taken by the Coast Guard against MTSA-Regulated Facilities</b>	<b>41</b>
<b>Appendix V</b>	<b>Acknowledgments of Agency and Private Sector Contributors</b>	<b>44</b>

---

<b>Appendix VI</b>	<b>Comments from the Department of Homeland Security</b>	45
--------------------	--	----

---

<b>Appendix VII</b>	<b>GAO Contacts and Staff Acknowledgments</b>	46
	GAO Contacts	46
	Acknowledgments	46

---

<b>Related GAO Products</b>		47
-----------------------------	--	----

---

## Tables

Table 1: Type of Security Enhancements the 10 Chemical and 8 Water Facilities We Visited Reported Making Since September 11	21
Table 2: Existing Industry Initiatives and Federal Security Requirements Imposed on Chemical, Water, and Maritime Facilities	27
Table 3: Number of Community Water Systems by Ownership and Population Service Category for Fiscal Year 2004	38
Table 4: Responsible Care® Security Code Deadlines for ACC Facilities	39
Table 5: Responsible Care® Security Code Deadlines for SOCMA Facilities	40
Table 6: Enforcement Actions Taken between July 1, 2004, and December 31, 2004, by Regulatory Citation Topic	43

---

## Figures

Figure 1: A Chemical Facility	10
Figure 2: A Community Water System	11
Figure 3: A Maritime Facility	12
Figure 4: Examples of Perimeter and Access Controls Chemical Facilities Reported Implementing	21
Figure 5: A Risk Management Cycle	24

---

---

## Abbreviations

ACC	American Chemistry Council
AMWA	Association of Metropolitan Water Agencies
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
MTSA	Maritime Transportation Security Act of 2002
NAWC	National Association of Water Companies
NRWA	National Rural Water Association
SOCMA	Synthetic Organic Chemical Manufacturers Association

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. 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, DC 20548

March 28, 2005

The Honorable Robert C. Byrd  
Ranking Member, Subcommittee on Homeland Security  
Committee on Appropriations  
United States Senate

Dear Senator Byrd:

The USA PATRIOT Act defined critical infrastructure as those “systems and assets . . . so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”<sup>1</sup> We often take these systems for granted because they are so basic in our daily lives that we generally only notice them when their service is disrupted. The National Strategy for Homeland Security grouped the critical infrastructure of the United States into 13 sectors—agriculture, banking and finance, chemical, defense industrial base, emergency services, energy, food, government, information and telecommunications, postal and shipping, public health, transportation, and water sectors. Further, the President designated a lead agency for each of the 13 sectors to coordinate interaction between the federal government and the private sectors. The lead agency for the chemical sector is the Department of Homeland Security (DHS) and the lead agency for the water sector is the Environmental Protection Agency (EPA).

In this report, we focus on the chemical and water sectors and on maritime facilities within the transportation sector. These three sectors include a variety of vital assets. Although the total number of chemical sector facilities is not clear, there are many facilities that manufacture chemicals. There are about 15,000 facilities—including chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals the EPA has estimated pose the greatest risk to human health and the environment. Of these 15,000 facilities, DHS estimates there are about 4,000 chemical manufacturing facilities. There

---

<sup>1</sup>Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 401 (2001).

---

are approximately 53,000 community drinking water systems and more than 2,900 maritime facilities that are required to comply with certain provisions of the Maritime Transportation Security Act of 2002 (MTSA).<sup>2</sup>

Terrorist attacks, such as the theft of certain chemicals or contamination of our water at chemical, water, or maritime critical infrastructure facilities, could have a significant impact on the health and safety of millions of Americans and result in environmental damage or disruption to the economy. This report responds to your request that we describe the actions that the private sector is taking to secure its critical assets in chemical, water, and maritime facilities. We are providing information on the following questions: (1) What federal requirements exist for the chemical and water sectors to secure their facilities and what federal efforts were taken by the lead agencies for the chemical and water sectors to facilitate these sectors' actions? (2) What actions have the chemical and water sectors reported taking to address security vulnerabilities and what, if any, obstacles did they say they faced in implementing security measures? (3) To what extent do the chemical and water sectors' actions reflect a risk management approach? (4) How do the chemical and water sectors perceive the role of the federal government in protecting these facilities? (5) What are the results of the Coast Guard's compliance inspection program to ensure that maritime facilities implemented security enhancements as required by the MTSA and what actions has the Coast Guard taken to ensure that its program is effective?

To address our five objectives, we reviewed pertinent federal legislation, implementing regulations, and agency guidance on facility security and met with DHS and EPA officials. We also met with industry representatives from the American Chemistry Council (ACC) and the Synthetic Organic Chemical Manufacturers Association (SOCMA),<sup>3</sup> the two

---

<sup>2</sup>Pub. L. No. 107-295, 116 Stat. 2064 (2002). According to the Coast Guard, 238 MTSA-regulated maritime facilities handle "bulk liquid chemicals."

<sup>3</sup>The ACC is a trade association that represents approximately 140 companies that operate approximately 2,000 facilities that encompass more than 85 percent of the productive capacity for the manufacture of basic chemicals in the United States. SOCMA is a trade association that represents approximately 160 companies that manufacture specialty or custom chemicals in the United States. Thirty-six of SOCMA's member companies are also members of the ACC. The remaining 124 SOCMA members operate 273 facilities in the United States. Both associations require their members to abide by the Responsible Care® Security Code, which lays out a process for facility operators to help secure against the threat of terrorism. ACC has also lobbied Congress regarding the need for federal regulation for chemical plant security.

---

principal U.S. chemical industry associations; the Association of Metropolitan Water Agencies (AMWA),<sup>4</sup> representing public water systems; 10 chemical facilities that were members of ACC or SOCMA; and 8 community water systems, 5 public and 3 private. We also obtained information from the National Association of Water Companies (NAWC), which represents privately owned water systems and the National Rural Water Association (NRWA).<sup>5</sup> In conducting our work in the water sector, we focused on community water systems—public water systems that supply water to the same population year-round—since the primary focus of critical infrastructure efforts in the water sector is on these systems. Seven of the 10 chemical facilities we visited are located on navigable waterways and are also regulated by the Coast Guard under the MTSA. We included chemical facilities from which a chemical release, resulting from an attack, could have a severe impact on surrounding communities. To assist us in selecting these facilities, we relied upon assessments completed by ACC and SOCMA members regarding the impact of a potential chemical release at its facilities. In conducting our work on the chemical sector, we focused on actions taken to strengthen security at a selected facility. We did not address actions taken by facility personnel to protect the transport of chemicals from the facility to other locations by way of various transport mechanisms such as rail cars or tank trucks nor did we address actions taken by facility personnel to prevent the sale of hazardous chemicals to terrorists masquerading as bona fide customers. The 8 community water systems we chose served a range of populations and were selected from systems that were subject to drinking water security and safety requirements of the Public Health Security and

---

<sup>4</sup>AMWA has nearly 200 member agencies that collectively serve 120 million Americans. AMWA functions as the voice for the largest publicly owned drinking water systems on regulatory, legislative, and security issues.

<sup>5</sup>NAWC is the only national trade association representing the private and investor-owned water utility industry that provides drinking water to 22 million Americans. NAWC serves as a mechanism for its members to respond to federal legislative and state regulatory initiatives that broadly affect the industry, including security-related initiatives. NRWA is a nonprofit federation of state rural water associations that provides support services to more than 24,550 water and wastewater utilities. NRWA's Board of Directors is composed of elected board members from each state association. NRWA programs include technical assistance to rural and small community water systems (1) on the design and implementation of ground water source water protection plans, (2) Safe Drinking Water Act compliance issues, (3) health protection related to public-drinking water, and (4) other managerial, financial and operational issues.



---

Bioterrorism Response Act of 2002 (Bioterrorism Act).<sup>6</sup> We also interviewed Coast Guard officials in headquarters and five local Coast Guard Marine Safety Offices and reviewed Coast Guard data and documents regarding the Coast Guard's efforts to complete compliance inspections of facilities covered by MTSA, enforcement actions and operational controls taken, and efforts to ensure the effectiveness of the inspection program. Information gathered from the 10 chemical and 8 water facilities we visited are illustrative, are not statistically representative of their respective industry as a whole, and therefore should not be considered to represent the views of the sectors as a whole.

We conducted our work in accordance with generally accepted government auditing standards from October 2004 through March 2005. Appendix I includes more detailed information on our scope and methodology.

---

## Results in Brief

Few federal requirements address security in the chemical and water sectors. However, the government has provided financial and other types of assistance to help these sectors implement security improvements. The federal government has enacted some legislation in these sectors to help prevent accidental releases of hazardous materials. For example, the Emergency Planning and Community Right to Know Act requires, in general, certain facilities to participate with local emergency planning committees that develop emergency response plans in the event of an accidental release of hazardous material.<sup>7</sup> With the enactment of the Bioterrorism Act of 2002, the federal government provided legislation to secure community water systems that serve more than 3,300 people, including systems that store various chemicals, against intentional attacks. This act requires operators of community water systems to perform vulnerability analyses of their facilities and to prepare or update an existing emergency response plan. MTSA and its implementing regulations require maritime facility owners and operators, including chemical

---

<sup>6</sup>Pub L. No. 107-188, 116 Stat. 594 (2002). Provisions of this act require drinking water systems serving more than 3,300 people to complete vulnerability assessments by certain dates depending upon the population size served. For example, systems serving a population greater than 3,300 but less than 50,000 were to complete such assessments by June 30, 2004. The act further required systems to prepare or revise an emergency response plan incorporating the results of the vulnerability assessment within 6 months after completing the assessment.

<sup>7</sup>Pub. L. No. 99-499, 110 Stat. 1728 (1986).

---

facilities, to conduct assessments of their facilities to identify vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement the measures discussed in the security plans. Other federal actions taken by DHS and EPA to assist the chemical and water sectors include providing financial assistance in the form of grants, threat information and guidance, training and exercises, and infrastructure protection initiatives, as well as setting security requirements for some facilities and reviewing actions by maritime facilities to determine compliance with MTSA.

Chemical facilities and community water systems reported making security improvements separate from federal requirements. The chemical industry's principal trade associations, the American Chemistry Council and the Synthetic Organic Chemical Manufacturers Association, adopted the Responsible Care® Security Code in 2002; it requires their member companies to perform vulnerability assessments, develop plans to mitigate vulnerabilities, take actions to implement the plans, and undergo a third-party verification that facilities implemented identified physical security enhancements. All 10 of the chemical facilities we visited reported making significant progress in fulfilling the requirements of the security code. Other facilities that use chemicals also have developed security initiatives on their own, some of which are modeled after the Responsible Care® Security Code. Although the water sector has not generated a specific industry code, the eight community water systems we visited were all regulated under the Bioterrorism Act, which requires systems to, among other things, perform vulnerability analyses of their facilities and prepare or update an existing emergency response plan with respect to intentional attacks. All eight of the community water systems we visited reported that they had completed their vulnerability assessments as well as implemented additional enhancements not required under the Bioterrorism Act, such as increasing access controls. Despite progress being made to enhance security, officials at both the chemical facilities and community water systems we visited reported encountering obstacles in making security enhancements and maintaining a level of security consistent with their needs. For example, officials at three chemical facilities reported experiencing difficulties, such as delays in obtaining permits or other approvals needed from federal authorities to install fences to better protect the perimeter of their chemical facilities. Officials at six of the community water systems we visited reported economic constraints, such as balancing the need for rate increases to fund security enhancements with efforts to keep rates low.

---

Through federal regulations and private sector efforts, chemical facilities that are members of the chemical industry's principal trade associations and the drinking water sector have incorporated some elements of a risk management framework to improve their security since September 11. A risk management framework includes assessing risk, evaluating alternatives for reducing risks, prioritizing which of those alternatives to implement, monitoring their implementation, and continually using new information to adjust actions taken. Information about risks is central to determining which security enhancements should be implemented based on available resources. Although the chemical sector's security efforts are not regulated, the chemical industry's principal trade associations require their members, as a condition of membership, to follow a security code. While the code incorporates elements of a risk management framework, the proportion of total chemical facilities within the chemical sector that adhere to the code is uncertain. About 2,300 ACC and SOCMA chemical manufacturing facilities follow the Responsible Care® Security Code; 1,100 of which are among the 15,000 facilities—including chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment. Within these 15,000 facilities, DHS estimates there are about 4,000 chemical manufacturing facilities. In March 2003, we recommended that the Secretary of Homeland Security and the Administrator of EPA jointly develop, in consultation with the Office of Homeland Security a comprehensive national chemical security strategy to include, among other things, information on industry security preparedness and a legislative proposal to require chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action.<sup>8</sup> At that time, DHS and EPA agreed that legislation requiring chemical facilities to assess and address vulnerabilities to terrorist attack should be enacted.

The water sector is regulated by the Bioterrorism Act of 2002, which requires community water systems serving more than 3,300 people to, among other things, perform vulnerability analyses of their facilities. The community water systems we visited implemented enhancements not required under the act, although actions were limited by their own resource constraints. The nation's drinking water systems are not required

---

<sup>8</sup>See 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.: March 2003).

---

to implement any risk reduction actions based on their vulnerability assessments or report to EPA on measures that have been implemented. Thus, the extent of the actions taken by these water systems is unknown. However, the Conference Report accompanying the Department of Homeland Security Appropriations Act for fiscal year 2005 calls for DHS to analyze whether it should require private sector entities to provide it with information concerning these entities' security measures and vulnerabilities to improve DHS's ability to evaluate critical infrastructure protections nationwide.<sup>9</sup> This report also mandates that GAO review DHS's analysis when it is complete. A DHS official has told us that it preliminarily expects to complete this analysis in December 2005.

In February 2005, DHS released its interim National Infrastructure Protection Plan, which we have not fully evaluated. This plan outlines a risk management framework to guide future efforts to identify and protect critical infrastructure and defines the roles of federal, state, local, and tribal agencies and the private sector using elements of this framework.

Operators of chemical manufacturing facilities and community water systems we contacted agreed that the federal role should include communicating threat information but had different views with respect to the need for the government to enact additional regulation to enhance security protection. Officials at 8 of the 10 of the chemical facilities we visited reported that the federal government should introduce regulations comparable to the Responsible Care® Security Code for the entire chemical sector to follow. Officials at 3 of the facilities we visited stated that those facilities that do not adhere to the Responsible Care® Security Code may have a competitive advantage over those facilities that do adhere to the code. In comparison, the majority of officials at the community water systems we visited reported that the federal government should provide technical support and guidance to help the water sector in developing and implementing security enhancements. The majority of officials we interviewed also supported the need for the federal government to expand financial support for security enhancements in the water sector by providing funding designated for community water systems.

---

<sup>9</sup>H.R. Conf. Rep. No. 108-774, at 75 (2004) accompanying H.R. 4567, ultimately enacted into law as Pub. L. No. 108-334, 118 Stat. 1298 (2004).

---

The Coast Guard has found that the vast majority, or approximately 97 percent, of maritime facilities are in compliance with MTSA requirements. However, the Coast Guard has not yet determined the effectiveness of its MTSA compliance inspection process. The Coast Guard reported inspecting all of the more than 2,900 regulated facilities between July 1, 2004, and December 31, 2004, and taking 312 enforcement actions against facility owners or operators for noncompliance with MTSA requirements. In addition to taking the 312 enforcement actions, the Coast Guard imposed operational controls on 29 MTSA facilities, such as suspending certain facility operations. The Coast Guard has taken some actions to facilitate the effectiveness of its compliance program, such as developing detailed checklists for facility inspections and training its inspectors. However, because of the high priority given to complete inspections at all regulated facilities by December 31, 2004, the Coast Guard said it has not completed an evaluation of the overall effectiveness of the compliance inspections, but plans to incorporate lessons learned from such an evaluation in the future. In June 2004, we issued a report on the status of the Coast Guard's strategy for monitoring and overseeing the implementation requirements of MTSA. At that time, we recommended that the Coast Guard evaluate its initial compliance inspection efforts upon completion and use the results to strengthen the compliance process for its long-term strategy.<sup>10</sup> The Coast Guard agreed with our recommendation.

We provided a draft of this report to DHS and EPA for review and comment. DHS and EPA generally concurred with the contents of the report. A copy of DHS's letter commenting on the report is presented in appendix VI. EPA did not provide a formal letter.

---

## Background

The *National Strategy for Homeland Security and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* identified the private sector as the owner of 85 percent of the nation's critical infrastructure and recognized that the owners of this infrastructure bear primary responsibility for protecting their facilities from deliberate acts of terrorism. The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* specifically designated the role of the federal government, "to coordinate the complementary efforts and

---

<sup>10</sup>See GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, [GAO-04-838](#) (Washington, D.C.: June 2004).

---

capabilities of government and private institutions to raise our level of protection over the long term.” Moreover, the President issued a directive emphasizing the federal government’s role by designating the Secretary of Homeland Security to identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on those that could be exploited to cause catastrophic health effects or mass casualties.<sup>11</sup> The directive requires the Secretary to collaborate with other federal departments and agencies to develop a program to map critical infrastructure and key resources; model the potential implications of terrorist exploitation of vulnerabilities within the critical infrastructure and key resources; and develop a national indications and warnings architecture, among other things, to help identify indicators and precursors to an attack. This directive also required DHS to produce a comprehensive integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives by December 17, 2004.

Our report focuses on efforts in the chemical and water sectors and the maritime segment of the transportation sector. The chemical sector is diverse in that its facilities produce, use, or store a multitude of products including (1) basic chemicals used to manufacture other products such as plastics, fertilizers, and synthetic fibers; (2) specialty chemicals used for a specific purpose such as a functional ingredient or as a processing aid in the manufacture of a diverse range of products such as adhesives and solvents, coatings, industrial gases, industrial cleaners, and water management chemicals; (3) life science chemicals consisting of pharmaceuticals and pesticides; and (4) consumer products such as hair and skin care products and cosmetics. To produce and deliver these products, the sector depends on raw materials, manufacturing plants and processes, and distribution systems, as well as research facilities and supporting infrastructure services, such as transportation and electricity. Because many chemicals are inherently hazardous, the release of chemicals or the risk of contamination at chemical facilities poses a potential threat to public health and the economy. Figure 1 depicts a chemical facility.

---

<sup>11</sup>Homeland Security Presidential Directive Number 7 (Washington, D.C.: December 17, 2003).

---

**Figure 1: A Chemical Facility**



Source: American Chemistry Council.

The water sector consists of two basic components: freshwater supply and wastewater collection and treatment. As we previously mentioned, we focused on community water systems within supply since the primary focus of critical infrastructure efforts is on these systems. According to EPA data, in 2004, there were approximately 53,000 community water systems in the United States.<sup>12</sup> EPA's data reflect that ownership of these systems is evenly split—about half are publicly owned by state and local authorities and about half are privately owned.<sup>13</sup> According to EPA, the majority of the U.S. population gets its water from publicly owned systems

---

<sup>12</sup>EPA provided data on the number of drinking water systems in the United States, including those subject to the Bioterrorism Act, by extracting information from the agency's national database called the Safe Drinking Water Information System. EPA does not have data on the ownership of approximately 2 percent of these systems.

<sup>13</sup>According to EPA's data, a very small portion of community water systems (less than 1 percent) are federally owned.

---

(see app. II for more details on the number of community water systems in the United States). Community water systems vary by size and other factors but most typically include a supply source, such as a reservoir; a treatment facility, which stores and uses chemicals, such as chlorine, to eliminate biological contaminants; and a distribution system, which includes water towers, piping grids, pumps, and other components to deliver treated water to consumers. Community water systems often contain thousands of miles of pipes and numerous access points that can be vulnerable to terrorist attack. Figure 2 reflects a community water system.

**Figure 2: A Community Water System**



Source: U.S. Army Corps of Engineers.

Maritime facilities include a number of waterfront facilities such as container terminals, factories, and shipping terminals, which may contain hazardous materials, as well as passenger terminals. In addition to possessing the potential for being used as a conduit for smuggling weapons of mass destruction or other dangerous materials into the country, maritime facilities present attractive targets of opportunity for terrorists to impact the nation's economy. Figure 3 depicts a maritime facility.



---

**Figure 3: A Maritime Facility**



Source: GAO.

---

## Few Federal Security Requirements Exist for the Chemical and Water Sectors, but Other Federal Actions Have Facilitated these Sectors' Efforts to Enhance Security

Currently, few federal requirements specifically address the security of chemical or drinking water systems from terrorism. Some federal requirements have been enacted to help prevent and mitigate accidental releases of hazardous chemicals. For example, the Emergency Planning and Community Right to Know Act requires, in general, certain facilities to participate with local emergency planning committees that develop emergency response plans in the event of an accidental release of hazardous material. Additionally, the 1990 Clean Air Act Amendments<sup>14</sup> require certain chemical facilities to develop risk management plans to help prevent accidental releases of hazardous air pollutants. Under this act, EPA requires that about 15,000 facilities—including chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals posing the greatest risk to human health and the environment take a number of steps to prevent and prepare for an

---

<sup>14</sup>Pub. L. No. 101-549, 104 Stat. 2399 (1990).

---

accidental chemical release.<sup>15</sup> Specifically, EPA regulations implementing the Clean Air Act require that the owners and operators of chemical facilities include a facility hazard assessment, an accident prevention program, and an emergency response program as part of their risk management plans. The Bioterrorism Act was enacted to specifically help secure community water systems that provide water to more than 3,300 people, including such systems' storage of various chemicals, against purposeful attacks.<sup>16</sup> It requires operators of community water systems to perform vulnerability analyses of their facilities and to prepare or update an existing emergency response plan. 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.

Although the federal government does not have primary responsibility for implementing security enhancements at privately owned critical infrastructure, DHS and EPA—the lead agencies for the chemical and water sectors respectively—have taken some actions to try to facilitate private sector security improvements by (1) providing financial assistance, (2) providing information and guidance, (3) providing training and exercises, (4) developing infrastructure protection initiatives, (5) setting security requirements for some facilities and related deadlines for taking required measures, and (6) reviewing actions taken at those facilities.

- *Providing financial assistance:* The federal government has provided financial assistance through several grant programs such as port security grants,<sup>17</sup> EPA's security planning grant program for vulnerability

---

<sup>15</sup>These facilities are known as Risk Management Plan, or RMP, facilities. The federal government has identified 140 toxic and flammable chemicals that, in certain amounts, would pose the greatest risk to human health and the environment if they were accidentally released into the air. See GAO-03-439 (Washington, D.C.: March 2003) for a more complete listing of the provisions related to an accidental release under the Clean Air Act.

<sup>16</sup>In 2003, EPA officials stated that approximately 2,000 Risk Management Plan chemical facilities may be covered under the Bioterrorism Act.

<sup>17</sup>Port security grants are awarded to critical national seaports and facilities to enhance facility and operational security. They were originally administered by the Transportation Security Administration (TSA) in coordination with the Maritime Administration and the Coast Guard. These grants are currently administered by the Office of State and Local Government Coordination and Preparedness in DHS.

---

assessments,<sup>18</sup> and the Homeland Security Grant Program<sup>19</sup> for infrastructure security. For example, 4 of the 10 chemical facilities we visited reported receiving port security grants ranging from \$265,000 to \$1.8 million that helped to defray the costs they incurred in implementing security enhancements since September 11, which ranged from \$2.3 million to \$10 million.<sup>20</sup>

- *Information sharing and guidance:* DHS and EPA partner with the chemical and water sectors' Information Sharing and Analysis Centers to coordinate and establish information-sharing mechanisms on critical infrastructure protection that includes threat information.<sup>21</sup> As we reported in January 2005, DHS is also seeking to enhance communication between critical infrastructure sectors, like the chemical and water sectors, with the government.<sup>22</sup> For example, it established a Water Sector Coordinating Council that consists of representative members of the water sector community and is charged with identifying information and other needs of the sector, including the appropriate use of and the relationships among the Water Information Sharing and Analysis Center, the Water Security Channel, and the Homeland Security Information Network—a national communication mechanism that is to provide the water sector with a suite of information and communication tools to share critical information

---

<sup>18</sup>Security planning grants were administered by EPA through August 2002 to provide assistance to publicly and privately owned community drinking water systems serving 100,000 people or more. Under this program, EPA allowed up to \$115,000 to each utility to develop or revise a vulnerability assessment, emergency response or operating plan, security enhancement plans and designs, or a combination of these efforts. In commenting on this report, EPA officials also told us that they used \$20 million from their 2002 supplemental appropriation to provide funds to (1) states to facilitate small and medium-sized community water systems' (that is, that served more than 3,300 but less than 100,000 people) efforts to obtain technical assistance related to the development of vulnerability assessments and emergency response plans as required by the Bioterrorism Act and (2) to organizations providing such assistance.

<sup>19</sup>Homeland security grants are a series of grants designed to support critical state and local missions, including the preparedness of first responders and citizens, public health, infrastructure security, and other public safety activities. These grants are administered by the Office of State and Local Government Coordination and Preparedness, the Federal Emergency Management Agency, and TSA.

<sup>20</sup>The 10 chemical facilities we visited reported spending between \$1 million and \$10 million to enhance security since September 11.

<sup>21</sup>See GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 2004).

<sup>22</sup>See GAO, *Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security*, GAO-05-165 (Washington, D.C.: January 2005).

---

within the sector, across other sectors, and with DHS.<sup>23</sup> According to a DHS official, the department is assembling a Government Coordinating Council made up of federal, state, and local officials to assess impacts across critical infrastructure sectors, including the water sector. A DHS official also told us that a similar Government Coordinating Council for the chemical sector was formed on March 17, 2005. For maritime facilities, the Coast Guard established local port security committees known as Area Maritime Security Committees to, among other things, serve as a link for communicating threats and disseminating appropriate security information to port stakeholders such as facility owners or operators. Required under MTSA, these committees are headed by a Coast Guard officer and are composed of a wide range of port stakeholders including members from law enforcement agencies, maritime industry (which could include chemical facilities on the waterfront), and federal, state, and local governments. DHS and EPA have also provided guidance to the chemical and water sectors, respectively, for conducting risk assessments.<sup>24</sup> In addition, EPA provides technical assistance to the water sector to help ensure the continued security of the nation's drinking water. For example, trained environmental professionals, scientists, and engineers provide information on technological advances in water security. EPA prepared voluntary guidelines—the *Interim Final Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems*—for drinking water systems to use to help plan for and respond to intentional threats and incidents related to water contamination. EPA also established a Water Security Working Group made up of 16 members from the wastewater and drinking water utilities and environmental and rate-setting organizations. The group advises the National Drinking Water Advisory Council (NDWAC)<sup>25</sup> on ways to address several specific security needs of the sector. The working group is to identify features of an active and effective security program and ways to measure the adoption of these practices and provide recommendations to NDWAC by the spring of 2005. The working group is also charged with identifying incentives for the voluntary adoption of an active and effective security program in the drinking water and wastewater sector. In turn,

---

<sup>23</sup>In November 2004, the Water Information Sharing and Analysis Center launched a free security advisory system known as the Water Security Channel to distribute federal advisories on security threats via e-mail to the water sector.

<sup>24</sup>EPA also developed guidance for community water systems to use in developing or revising their emergency response plans as required by the Bioterrorism Act.

<sup>25</sup>The council is made up of 15 members who are appointed by EPA's Office of Ground Water and Drinking Water, and serve staggered 3-year terms.

---

NDWAC provides advice and recommendations to EPA related to drinking water quality, including water security and emerging issues on drinking water.

- *Training and exercises:* DHS and EPA have also provided a series of specialized security training courses to assist the private sector in protecting its critical assets. For instance, DHS has provided training programs to first responders and facility security officers to better equip these personnel with appropriate skills to prevent and protect against continuing and emerging threats to the nation's critical infrastructure. Additionally, EPA has sponsored a variety of training courses, meetings, workshops, and webcasts to help enhance the security and emergency response capabilities of drinking water facilities. DHS has also initiated several security exercises with individual facilities and held portwide exercises or drills initiated by the Coast Guard to help these facilities react appropriately in the event of a terrorist attack.
- *Infrastructure protection initiatives:* Two initiatives that DHS has under way to facilitate efforts by the private sector to enhance critical infrastructure protection are the Buffer Zone Protection Program and Site Assistance Visits. As part of the Buffer Zone Protection Program—a program designed to reduce specific vulnerabilities by developing protective measures that extend from the critical infrastructure site to the surrounding community—DHS provides advice and guidance to state and local partners as they prioritize specific vulnerability reduction efforts. DHS also conducts site assistance visits at critical infrastructure sites nationwide to address key areas of concern at facilities requiring security enhancements. DHS subject matter experts in the area of physical security measures, system/interdependencies, and terrorist attack planning conduct these visits (which generally last 1 to 3 days) in which, among other things, the vulnerabilities of the site or facility are identified and mitigation options are discussed. The site assistance visits also provide insight into threats that pertain to the sector based on DHS's access to threat information.
- *Setting security requirements and deadlines:* In October 2003, the Coast Guard issued regulations to enforce MTSA's security requirements for maritime facilities, including some chemical facilities in proximity to waters subject to U.S. jurisdiction. These regulations established a process and related deadlines for maritime facilities to follow in assessing their security risks and preparing related plans to include actions mitigating any identified vulnerabilities.

- 
- *Reviewing actions taken:* In 2004, the Coast Guard began a compliance inspection program with on-site inspections and spot checks to help ensure compliance by MTSA-regulated facilities.

As part of its efforts to coordinate with the chemical sector to enhance critical infrastructure protection as discussed above, DHS gathered data on actions taken by some chemical facilities. However, DHS officials told us that these data do not reflect actions taken by the entire chemical industry. In addition, EPA officials told us that while engaged in meetings and technical assistance or training sessions with community water systems, they received information on actions taken by some community water systems. However, they also stated that this information was anecdotal and does not reflect actions taken by the entire water sector.

---

## Chemical Facilities and Water Systems Reported Taking Actions to Address Security Vulnerabilities but Said They Faced Obstacles in Implementing Security Measures

One of the chemical industry's principal trade associations, ACC, set policy for its members to follow that was designed to strengthen infrastructure protection at its members' facilities, whereas, the water sector followed the requirements of legislation. While the chemical and water facilities we visited reported taking a variety of actions to strengthen the security of their facilities; they also identified obstacles both in making these enhancements and in maintaining them.

---

## Chemical Facilities and Water Systems We Visited Reported Making Security Enhancements Separate from Federal Regulations

After September 11, the chemical and water sectors reported taking a variety of actions to strengthen the security of their facilities. Prior to September 11, ACC, SOCMA, and the Chlorine Institute initiated the development of *Site Security Guidelines* for its members to help facility managers make decisions on appropriate security measures based on risk that were subsequently published in October 2001. In 2002, ACC adopted a

---

security code to accompany its Responsible Care Management System®.<sup>26</sup> As a condition of membership, ACC requires its members to adhere to its Responsible Care® Security Code. Under the Responsible Care® Security Code, member companies are to perform vulnerability assessments, develop plans to mitigate vulnerabilities, take actions to implement the plans, and undergo third-party verification that the facilities implemented identified physical security enhancements. While the Responsible Care® Security Code does not require third parties to verify that a vulnerability assessment was conducted appropriately or that actions taken by a facility adequately address security risks, the Responsible Care Management System® certification requirements do require member companies to periodically conduct independent third-party audits that include an assessment of their security programs and processes and implementation of corrective actions. SOCMA also adopted the Responsible Care® Security Code, requiring its members to adhere to it as well. (For more details regarding the Responsible Care® Security Code and the status of ACC and SOCMA members' actions, see app. III).

In June, 2004, the chemical industry confirmed to DHS that it had established the Chemical Sector Council to act as a coordination mechanism for the chemical sector to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures and best practices. The Chemical Sector Council is composed of 15 sector associations: ACC, the American Forest and Paper Association, the Chemical Producers and Distributors Association, the Chlorine Chemistry Council, the Compressed Gas Association, Crop Life America, the Institute of Makers of Explosives, the International Institute of Ammonia Refrigeration, the National Association of Chemical Distributors, the National Paint and Coatings Association, SOCMA, the Adhesive and Sealant Council, the Chlorine Institute, the Fertilizer Institute, and the Society of the Plastics Industry, Inc.

In March 2003, we reported that other facilities that use chemicals, including fertilizer suppliers, petroleum and natural gas facilities, food storage facilities, water treatment facilities, and wastewater treatment facilities, have developed their own security initiatives.<sup>27</sup> For example, the

---

<sup>26</sup>In 1988, the ACC initiated Responsible Care®, which is a comprehensive management system for its members to follow to continuously improve safety performance; to increase communication; and to protect employees, communities, and the environment.

<sup>27</sup>See [GAO-03-439](#).

---

Fertilizer Institute, which represents fertilizer manufacturers and fertilizer retail and distribution facilities, developed a security code modeled after ACC's Responsible Care® Security Code. The Fertilizer Institute's code encourages facilities to develop vulnerability assessments and implement plans based on the assessments.

However, because the total number of facilities within the chemical sector is uncertain, it is difficult to determine the proportion of all chemical sector facilities that are not members of ACC or SOCMA and thus are not required to adhere to the Responsible Care® Security Code. For example, there are approximately 2,300 ACC and SOCMA facilities, 1,100 of which are among the 15,000 facilities—including, chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment. Within these 15,000 facilities, DHS estimates that there are about 4,000 chemical manufacturing facilities. A DHS official told us that the department is working with Argonne National Laboratory on the development of a taxonomy—a list of the types of facilities that should be included—for each critical infrastructure sector, including the chemical sector.

Although the water sector has not generated a specific industry code, all community water systems that serve more than 3,300 people are subject to the drinking water security and safety requirements of the Bioterrorism Act. According to EPA data, in fiscal year 2004, there were approximately 53,000 community water systems in the United States, of which about 8,600 (16 percent) were required by the Bioterrorism Act to prepare vulnerability assessments for their systems. According to EPA officials, as of February 23, 2005, all community water systems that serve 50,000 or more people have submitted their vulnerability assessments to EPA; whereas, 92 percent of the smaller systems (those serving between 3,301 and 49,999 people) have submitted their vulnerability assessments. Under the Bioterrorism Act, community water systems that serve 100,000 or more people were required to submit their vulnerability assessments to EPA by March 31, 2003; those systems that served between 50,000 and 99,999 people were required to submit their vulnerability assessments to EPA by December 31, 2003; and those that served between 3,301 and 49,999 people were required to submit their assessments by June 30, 2004.

The actions the facilities we visited reported taking reflect, in many ways, the security initiatives issued from trade industry associations and legislation enacted by the federal government. For example, all 10 of the chemical facilities we visited reported fulfilling the steps under the



---

Responsible Care® Security Code by completing their vulnerability assessments and developing plans to mitigate vulnerabilities.<sup>28</sup> Eight of those facilities reported that they have fully implemented their planned enhancements. The remaining two chemical facilities reported making significant progress on planned enhancements. However, they also reported implementing alternative measures for some enhancements, such as adding guards for additional patrols while permanent barriers are being constructed. In the water sector, officials at eight community water systems that we visited reported that they completed their vulnerability assessments in accordance with the Bioterrorism Act. Even though not specifically required by the Bioterrorism Act, officials at the eight community water systems we visited told us they implemented a number of enhancements, such as increasing access controls by establishing an electronic key control system that assigns keys to individual staff members and tracks their use. Table 1 provides additional information on the types of enhancements the chemical and water facilities reported taking since September 11, and figure 4 provides examples of some of these enhancements.

---

<sup>28</sup>The Responsible Care® Security Code directs chemical companies to perform vulnerability assessments of their facilities using methodologies developed by either Sandia National Laboratories or the Center for Chemical Process Safety (or another equivalent methodology). Sandia National Laboratories are multiprogram oriented and primarily address national defense issues. Sandia security experts developed the risk-based assessment methodology under sponsorship from the Department of Justice. The Center for Chemical Process Safety is a component of the American Institute of Chemical Engineers that, as part of its work on chemical safety, has developed vulnerability assessment methodology and offers courses and a certificate in security vulnerability analysis. SOCMA also developed a Chemical Site Security Vulnerability Analysis Model to provide chemical facilities with another mechanism for conducting site vulnerability analysis.

**Table 1: Type of Security Enhancements the 10 Chemical and 8 Water Facilities We Visited Reported Making Since September 11**

Type of security enhancement	Number of chemical facilities	Number of community water systems	Examples of enhancements
Increasing perimeter control	10	8	Fencing, gates, cameras, and signs
Increasing access control	10	8	Turnstiles, access control cards, and changing outer locks
Enhancing monitoring	10	7	Motion detectors and contamination detectors
Establishing system redundancies	5	5	Backup pumps, power systems, and storage capacity
Increasing automated (cyber) system protections	9	7	Separation of business and control process networks and firewalls
Increasing facility precautions	N/A	7	Shredding old facility maps
Making process or inventory changes	7	N/A	Reducing the inventory of hazardous chemicals stored on site

Source: GAO analysis of enhancements the chemical facilities and community water systems reported taking.

**Figure 4: Examples of Perimeter and Access Controls Chemical Facilities Reported Implementing**



Source: American Chemistry Council.

Note: From left to right: entrance barricades, card-code turnstile, and closed-circuit camera.

---

## Chemical Facilities and Water Systems Said They Faced Several Obstacles in Making and Maintaining Security Enhancements

In making security enhancements and in maintaining a level of security consistent with their needs, officials at the chemical facilities and community water systems we visited told us that they faced several obstacles. However, the obstacles varied by sector. Three chemical facility operators told us that they experienced difficulties in obtaining permits or approval from the U.S. Army Corps of Engineers to install fences to better protect the perimeter of their chemical facilities. Officials at one facility stated that they did not obtain a permit from the Army Corps of Engineers to install a fence on wetlands in a timely manner, while an official at another chemical facility said that they moved the planned location of their fenceline rather than go through a permitting process. The official representing the third chemical facility told us that they moved their fence line because the Corps of Engineers refused to allow them to install fences on the Corps-managed property. One of the United States Army Corps of Engineers' missions is to preserve wetlands. Project proponents who seek to fill in wetlands or waters are required under federal law to obtain a permit from the Army Corps of Engineers before they can undertake such activities. According to the Army Corps of Engineers, the agency requires permit applicants to avoid, minimize, or mitigate impacts to wetlands or waters in most cases.<sup>29</sup>

Officials from two other chemical companies we visited said that they were experiencing continuing difficulties in gaining cooperation from railroads to maintain security when railroad personnel made deliveries or picked up products from the chemical facilities' premises. An official from one of these chemical companies said that the railroads followed security standards that were lower than the chemical company's standards and often took actions that compromised the chemical facility's security. Officials representing two of the chemical facilities we visited also stated that they were challenged in obtaining contractors, such as crews hired to perform major system maintenance in the facilities, with an appropriate level of background screening.

Officials at six of the eight community water systems we visited stated that they faced economic constraints in addressing security issues, including insufficient financial resources to implement security enhancements and determining how best to use available funds given competing priorities

---

<sup>29</sup>In 2004, we reported that the Army Corps of Engineers approves virtually all such permit applications. See GAO, *Waters and Wetlands: Corps of Engineers Needs to Evaluate Its District Office Practices in Determining Jurisdiction*, [GAO-04-297](#) (Washington, D.C.: February 2004).

---

such as nonsecurity-related infrastructure upgrades. Officials at six of these systems told us that they are challenged to balance the need for rate increases to fund security enhancements with efforts to keep water rates low. Furthermore, officials at two community water systems stated that first responders such as police and firefighters were generally given priority to use DHS grant funds awarded to states in relation to homeland security. As a result, these community water officials said that within their states, the first responders typically consumed all of the grant funds and nothing remained for the utilities' use. DHS awards of homeland security grant funds, in general, have provided states with a certain measure of flexibility with respect to how grant funds are to be allocated and used by the states in support of their State Homeland Security Strategies.

Four of the eight community water systems we visited also stated that instituting a cultural change that stresses the importance of security was another challenge they needed to address. For example, an official at one of these systems said that its employees are not always diligent about carrying out security enhancements, such as ensuring that doors stay locked during shift changes. An official at another system noted that the public in his locality did not perceive the water system to be at risk and, if it was, the public believed that little could be done to prevent a terrorist attack, making it difficult for the community water system to obtain budget increases to pay for security enhancements. Officials at two of the eight community water systems we visited reported that sufficient technology was not available to ensure an appropriate level of security enhancements. For instance, one large community water system reported that while technology is currently available to allow a system to test its water supply for contaminants at a specific point in time, a readily accessible technology does not exist for continuously monitoring the supply that would alert a system immediately upon a contaminant's entry into the water. As reported in the fiscal year 2006 President's Budget, the Administration requested \$44 million to fund the Water Sentinel Initiative as a pilot program in five major cities. Under this initiative, the federal government would commence the development of a water surveillance system designed to enhance security of the nation's water supply by providing an early warning mechanism for possible contaminants, including chemical or biological agents, entering the water supply.

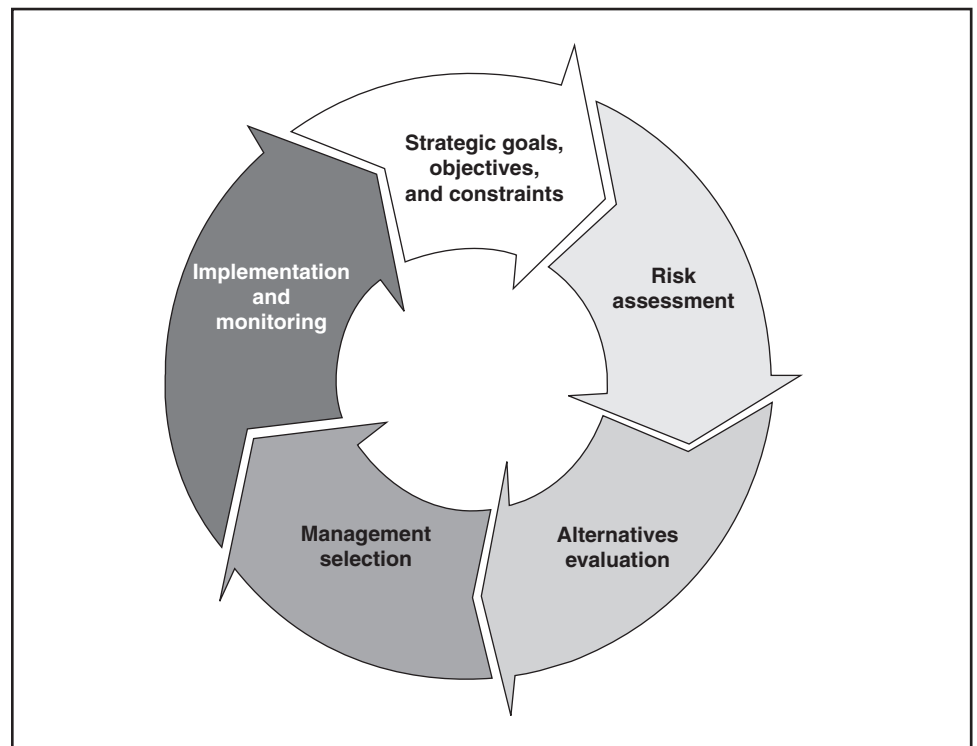
---

## The Chemical and Water Sectors Have Incorporated Some Elements of a Risk Management Framework to Address Their Security Vulnerabilities

The chemical and drinking water sectors have incorporated some elements of a risk management framework to protect their critical infrastructure. As shown in figure 5, 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. Adoption of a risk management framework can aid in assessing risk by determining which vulnerabilities should be addressed in what ways within available resources.

---

**Figure 5: A Risk Management Cycle**



Source: GAO.

Assessing risks for specific assets—such as community water systems or chemical plants on navigable waterways—is defined by two conditions: (1) probability, the likelihood, quantitative or qualitative, that an adverse

---

event would occur; and (2) consequences, the damage resulting from the event, should it occur.

Thus, the most severe risks are those that have both the greatest probability of occurring and would cause the greatest damage. Actual risk reflects the combination of the two factors. Risks may be managed by reducing the probability, the consequence, or, where possible, both.

As this suggests, identifying threats and vulnerabilities (e.g., weaknesses in structure or security operations) in existing infrastructure is necessary but not sufficient to fully manage the risks to the infrastructure. Assessing the vulnerability of infrastructure to damage or destruction should be coupled with an assessment of the probability that the vulnerability will be exploited and the consequences that would result if it were exploited. Several risks, each with equally serious potential consequences, may not be equally likely to occur. In addition, private entities may benefit from assistance in the form of risk information from intelligence or law enforcement agencies to assess the types of risks faced and the probability that these risks would result in an adverse event. Because it is unlikely that sufficient resources will be available to address all risks, it becomes necessary to prioritize both risks and the actions taken to reduce those risks, taking cost into consideration. For example, which actions will have the greatest net potential benefit in reducing one or more risks?

The information we obtained from our site visits and discussions with national chemical and water associations suggests that some elements of a risk management framework have been incorporated into the assessments and actions taken by both chemical and community water facilities. The chemical facilities we visited were all members of the ACC or SOCMA and subscribe to the Responsible Care® Security Code, which those associations require their members to follow.

Of the 2,300 ACC and SOCMA chemical facilities affected by the Responsible Care® Security Code, 1,100 are among the 15,000 facilities—including, chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment. As we previously mentioned, it is difficult to determine the proportion of chemical facilities that follow the Responsible Care® Security Code because even though DHS estimates that there are about 4,000 chemical manufacturing facilities within the 15,000 facilities, the total number of chemical facilities in the chemical sector is uncertain. In our March 2003 report, we recommended that the Secretary of Homeland Security and the

---

Administrator of EPA jointly develop, in consultation with the Office of Homeland Security, a comprehensive national chemical security strategy to include, among other things, information on industry security preparedness and a legislative proposal to require chemical facilities to expeditiously assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action.<sup>30</sup> DHS and EPA agreed that legislation requiring chemical facilities to assess and address vulnerabilities to terrorist attack should be enacted.<sup>31</sup>

Similar to the Responsible Care® Security Code, under MTSA and its implementing regulations, more than 2,900 maritime facilities (including some chemical) are required to assess risks, develop security plans to mitigate them, and implement those security plans. The Coast Guard is responsible for inspecting facilities for compliance.

The Bioterrorism Act requires all community water systems that serve populations of 3,300 or more to prepare vulnerability assessments and update or prepare emergency plans based on those assessments. EPA guidance for these vulnerability assessments calls for them to include (1) a characterization of the water system, (2) the identification of possible consequences of malevolent acts, (3) the critical assets subject to malevolent acts, (4) an assessment of the threat of malevolent acts, (5) an evaluation of countermeasures, and (6) a plan for risk reduction. However, as shown in table 2, community water systems are not subject to federal requirements to implement any risk reduction actions based on the completed vulnerability assessments or report to EPA on measures that have been implemented in a manner similar to that required of port facilities by MTSA. For those systems we visited, the actions taken reflected the systems' own risk assessments and resource constraints. Some systems have had more resources to devote to risk reduction than others.

Yet, the extent of actions taken by community water systems is unknown. The Conference Report accompanying the Department of Homeland Security Appropriations Act for fiscal year 2005 calls for DHS to analyze whether it should require private sector entities to provide it with information concerning these entities' security measures and

---

<sup>30</sup>See [GAO-03-439](#).

<sup>31</sup>At the time of this report, EPA was still the lead agency for the chemical sector. However, as previously mentioned, DHS is now the lead agency for the chemical sector.

vulnerabilities to improve DHS's ability to evaluate critical infrastructure protections nationwide. This report also mandates that GAO review DHS's analysis when it is complete. A DHS official has preliminarily told us that the Department expects to complete this analysis in December 2005.

**Table 2: Existing Industry Initiatives and Federal Security Requirements Imposed on Chemical, Water, and Maritime Facilities**

Security requirements	Elements of risk management			Third-party verification or compliance inspection
	Vulnerability assessment	Security or risk reduction plan	Implementation of measures	
Chemical Industry—ACC Responsible Care® Security Code <sup>a</sup>	X	X	X	X <sup>b</sup>
Bioterrorism Act <sup>c</sup>	X	<sup>d</sup>		
MTSA and the Coast Guard's implementing regulations <sup>e</sup>	X	X	X	X

Source: GAO analysis of above-mentioned legislation, guidance, and trade association code.

<sup>a</sup>This code applies to chemical facilities that are members of ACC and SOCMA.

<sup>b</sup>The Responsible Care® Security Code does not require that third parties verify that the vulnerability assessment was conducted appropriately or that actions taken by a facility adequately address security risks.

<sup>c</sup>This act and guidance apply to community water systems that serve more than 3,300 people. The act also requires such systems to prepare or update existing emergency response plans.

<sup>d</sup>Although not specifically required by the Bioterrorism Act, EPA guidance related to the preparation of vulnerability assessments required under the Bioterrorism Act calls for community water systems to include, among other things, a plan for risk reduction in their vulnerability assessments.

<sup>e</sup>This act, as implemented, generally applies to maritime facilities in proximity to navigable waters including facilities that handle explosive or other dangerous cargoes, liquefied natural gas or liquefied hazardous gas, or transfer oil or other hazardous materials; facilities that receive vessels certified to carry more than 150 passengers; facilities that receive certain passenger and cargo ships engaged in international voyages; facilities that receive certain foreign cargo vessels; and commercial barge fleeting facilities.

In February 2005, DHS released its Interim National Infrastructure Protection Plan, whose purpose is to “prioritize protection across [infrastructure] sectors, so that resources are applied where they offer the most benefit for reducing vulnerability, deterring threats, and minimizing



---

consequences of attacks.” Because we just recently received the plan, we have not fully evaluated it. However, the plan outlines (1) a risk management framework to guide future efforts to identify and protect critical physical infrastructure and (2) the roles of federal, state, local, tribal, and private agencies and entities in implementing this framework.

Under this approach, risks are to be managed in response to (1) specific threats and (2) plausible threats. Specific threats are situations where there is intelligence regarding targeted locations, sectors, or assets, or when there is suspected activity by groups known to favor attacks on certain types of assets. The likelihood of the threat would drive short-term protective measures. Plausible threats are those “that could logically occur and that would have negative consequences on a particular asset.” Plausible threats are treated as if all are equally likely to occur—that is, they result from the general threat environment. Thus, plausible threats focus protective efforts on the inherent vulnerabilities of different assets and the potential consequences of an attack, rather than the likelihood of a particular event.

The plan also outlines the roles and responsibilities of federal, state, local, and tribal agencies, and the private sector using elements of a risk management framework. The federal government’s role would include setting standards for identifying critical assets, assessing the most critical assets, developing consistent approaches and tools for identifying and assessing vulnerabilities, analyzing and disseminating threat information, promoting cross-sector best practices, tracking program implementation, and reporting on the national status of infrastructure assessment and protection. The role of state, local, and tribal agencies would include helping to identify assets, conducting and sharing assessments with the federal government, supplementing private sector capabilities in response to threats, developing state or local level strategies and best practices, and tracking performance where applicable. The private sector would play a role similar to that of state, local, and tribal agencies plus help to develop incentive programs for private entities.

---

## Officials at Chemical Facilities and Water Systems We Visited Agreed in Part about What the Federal Government's Role Should Be

Operators of 4 of the 10 chemical manufacturing facilities and seven of the eight community water systems we visited agreed that the federal role in protecting their facilities should include the transmittal of threat information. As we previously reported, to effectively communicate risks, experts suggest that threat information should be consistent, accurate, clear, and provided repeatedly through multiple methods; it should be provided in a timely fashion; and to the greatest extent possible, it should be specific about the potential threat.<sup>32</sup>

Officials representing the chemical facilities and community water systems we visited had fundamentally different views on other roles for the federal government. Officials representing 8 of the 10 chemical facilities we visited expressed the view that the federal government should introduce regulations and standards comparable to the Responsible Care® Security Code for the entire chemical sector to follow. Officials representing 3 of these facilities stated that those facilities that do not adhere to the Responsible Care® Security Code may have a competitive advantage over those facilities that do adhere to the code.

In comparison, only one of the eight water system operators we spoke with suggested the need for additional federal regulation. Rather, officials at four community water systems said they would like the federal government to establish security standards to guide actions for the water sector. Officials representing seven of the community water systems we visited said that they would like the federal government to expand support for security enhancements in the water sector by providing funding designated for community water systems. Moreover, officials at six of the community water systems we met with suggested that the federal government consistently emphasize the need for security for the sector and provide technical guidance on security planning. However, officials at four of the community water systems we met with said that they would prefer the federal government to refrain from issuing unfunded mandates. These officials elaborated that funding currently provided by the federal government was not sufficient to support federal requirements that the water companies complete vulnerability assessments. For example, officials at one large community water system said that their system

---

<sup>32</sup>See GAO, *Homeland Security: Communication Protocols and Risk Communication Principles Can Assist in Refining the Advisory System*, [GAO-04-682](#) (Washington, D.C. June 2004).

---

received an EPA grant that offset approximately 7 percent of the cost it incurred to perform its mandated vulnerability assessment.<sup>33</sup>

---

## The U.S. Coast Guard Completed Its Compliance Inspections and Plans to Review the Effectiveness of the Process

The U.S. Coast Guard has found that the vast majority, approximately 97 percent, of maritime facility owners or operators are meeting MTSA requirements. The Coast Guard reported completing compliance inspections at all 2,924 regulated facilities by December 31, 2004, resulting in 312 enforcement actions and operational controls imposed on 29 facilities. The Coast Guard reported taking these 312 enforcement actions against 98 facility owners or operators for violations. The most frequently cited deficiencies related to insufficient access controls; noncompliance by the owner or operator to ensure that the facility is operating in compliance with its facility's security requirements; noncompliance with facility security officer requirements, such as possessing the required security knowledge or carrying out all duties as assigned; and insufficient security measures for restricted areas. The Coast Guard's enforcement actions included issuing letters of warning or assessing monetary penalties for noncompliance. See appendix IV for more details on these enforcement actions. In addition to taking enforcement actions, the Coast Guard imposed operational controls, such as suspending certain facility operations, on 29 MTSA regulated facilities between July 1, 2004, and December 31, 2004, for identified deficiencies.

The Coast Guard has taken some actions to facilitate the effectiveness of its compliance inspection program for MTSA-regulated facilities, but it has not yet determined the overall effectiveness of the program. Some of the actions taken by the Coast Guard include conducting unscheduled spot checks in addition to scheduled inspections, developing detailed checklists for the inspectors to use during facility inspections, conducting reviews at both the local and national levels of the enforcement actions taken by the inspectors, and providing training for inspectors. However, Coast Guard officials said that because their priority was to complete the initial compliance inspections by December 31, 2004, they have not completed an evaluation of the effectiveness of the compliance actions for

---

<sup>33</sup>Officials at seven of the eight community water systems we visited reported tracking some cost information related to security enhancements implemented since September 11 that ranged from approximately \$23,000 to \$19 million. However, the cost information these officials provided is not precise, and as they told us it does not represent all costs incurred. Thus, the data should not be used to determine the cumulative costs incurred across all community water systems.

---

lessons learned that could be used to improve the inspection program in the future. The Coast Guard said that now that the initial surge of inspections has been completed, it plans to begin a systematic effort to evaluate the effectiveness of the compliance inspection program.

The Marine Safety Offices we visited also reported that evaluations of their compliance efforts have not yet been completed at the local level. Officials at these Marine Safety Offices stated that they anticipate taking a closer look at the results of the initial inspections to determine what improvements to make. Some of the measures they mentioned as ways to track the effectiveness of their compliance inspection activities included the recurrence of deficiencies previously identified during initial inspections or spot checks, the number of deficiencies identified during inspections or spot checks, and an index that tracks a facility's level of risk. In June 2004, we issued a report on the status of the Coast Guard's strategy for monitoring and overseeing the implementation requirements of MTSA. At that time, we recommended that the Coast Guard evaluate its initial compliance inspection efforts upon completion and use the results to strengthen the compliance process for its long-term strategy, clearly define inspector qualifications, and consider including unscheduled and unannounced inspections and covert testing.<sup>34</sup> The Coast Guard agreed with this recommendation.

---

## Agency Comments

We provided a draft of this report to DHS and EPA for review and comment. DHS provided formal written comments on a draft of this report on March 16, 2005, which are presented in appendix VI. In commenting on the draft report, DHS noted that it generally concurred with the report's contents and that the report presented generally valuable and useful information. DHS observed that the report did not mention efforts currently under way to improve government and private sector infrastructure protection coordination efforts through the formation of Government Coordinating Councils and Sector Coordinating Councils. We revised our report to include a discussion of the chemical and water sector Government Coordinating Councils and Sector Coordinating Councils. We are currently conducting another review of chemical facility security for the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, and are focusing on actions that DHS and other federal agencies have taken to improve chemical facilities' security. As part of this review, we are

---

<sup>34</sup>See [GAO-04-838](#).

---

identifying the efforts taken by the Chemical Sector Coordinating Council and the related Government Coordinating Council and will report on these issues at a later date.

EPA did not submit a formal letter but did provide comments. The comments expressed general agreement with the contents of the report. We also provided excerpts from our draft report to ACC, SOCMA, AMWA, NAWC, and NRWA for review and comment. DHS, EPA, ACC, SOCMA, and NAWC also offered specific technical comments and suggestions, which have been incorporated as appropriate.

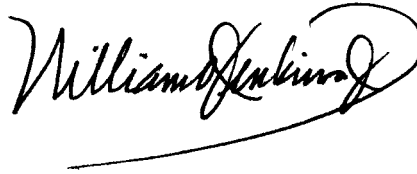
---

We plan no further distribution of this report until seven days after the date of this report. At that time, we will send copies of this report to the Senate Committee on Homeland Security and Governmental Affairs; Chairman, Subcommittee on Homeland Security, Senate Committee on Appropriations; House Committee on Government Reform; House Committee on Homeland Security; Subcommittee on Homeland Security, House Committee on Appropriations; the Secretary of Homeland Security, the Administrator of EPA, the Director, Office of Management and Budget and other interested parties. We will also make copies available to others on request.

---

In addition, this report will be available on GAO's Web site at <http://www.gao.gov>. If you or your staff have any questions about this report, please contact me at (202) 512-8777 or by e-mail at [jenkinswo@gao.gov](mailto:jenkinswo@gao.gov) or Debra Sebastian at (202) 512-9385 or by e-mail at [sebastiand@gao.gov](mailto:sebastiand@gao.gov). GAO contacts and staff acknowledgments are listed in appendix VII.

Sincerely yours,

A handwritten signature in black ink that reads "William O. Jenkins, Jr." The signature is written in a cursive style with a large, looping initial "W".

William O. Jenkins, Jr.  
Director, Homeland Security  
and Justice Issues

---

# Appendix I: Scope and Methodology

---

To determine federal security requirements for the chemical and water sectors and the efforts taken by the federal government to facilitate private sector protection of its critical assets, we met with Department of Homeland Security (DHS) and Environmental Protection Agency (EPA) officials, as well as representatives from the American Chemistry Council (ACC), the Synthetic Organic Chemical Manufacturers Association (SOCMA), the American Metropolitan Water Association (AMWA), 10 chemical facilities and 8 community water systems (the criteria used to select these facilities and systems are described below). We also obtained information from the National Association of Water Companies (NAWC) and the National Rural Water Association (NRWA). In addition, we reviewed pertinent federal legislation and implementing regulations and agency guidance on facility security for these sectors.

To determine actions officials in the chemical sector reported taking to enhance security of their facilities since September 11, the obstacles they faced in making such enhancements, and their perceptions of the role of the federal government in securing chemical facilities, we met with officials from ACC and SOCMA, and with officials from 10 chemical manufacturing facilities. We selected these facilities from those operated by members of ACC or SOCMA. To ensure that the facilities we visited were at greatest risk, and hence had the greatest need for security, we generally selected facilities from which a chemical release, stemming from an attack, would have a severe impact on surrounding communities. To assist us in selecting these facilities, we relied upon assessments completed by ACC and SOCMA members regarding the impact of a potential chemical release at its facilities. The facilities we selected produce petrochemicals, building block chemicals,<sup>1</sup> inorganic chemicals, plastics, and industrial gases. We also selected chemical facilities that were regulated by the Coast Guard under the Maritime Transportation Security Act (MTSA) and facilities that were not regulated to observe differences among these types of facilities. All facilities we selected were ACC or SOCMA members that volunteered to meet with us. We used a structured interview guide when questioning officials during our visits to these facilities. We did not verify that the security enhancements reported to us by the chemical facilities were actually taken. In conducting our work on the chemical sector, we focused on actions taken to strengthen security at a selected facility. We did not address actions taken by facility

---

<sup>1</sup>Building block chemicals are intermediary chemicals that are produced from raw materials and used in the production of other chemicals.

personnel to protect the transport of chemicals from the facility to other locations by way of various transport mechanisms such as rail cars or tank trucks nor did we address actions taken by facility personnel to prevent the sale of hazardous chemicals to terrorists masquerading as bona fide customers.

To determine actions the water sector officials reported taking to enhance security of their facilities since September 11, the obstacles they faced in making such enhancements, and their perceptions of the role of the federal government in securing community water facilities, we met with officials from the AMWA and with operators of eight community water systems.<sup>2</sup> We also obtained information from NAWC and NRWA. We selected systems from those that were regulated under the Bioterrorism Act—a federal law that addresses security matters with respect to community water systems. Three of the systems we selected were privately owned systems and five were publicly owned systems. For the publicly owned systems, we varied our selection to include systems that served a range of population sizes. Specifically, we selected three systems from those that served 100,000 or more people, one from those that served 50,000 to 99,999 people, and one from those that served 3,301 to 49,999 people. For the private sector systems, we selected one system that served approximately 3,500 people and two that served 100,000 or more.<sup>3</sup> In conducting our work in this area, we focused on water supply systems rather than wastewater treatment systems.<sup>4</sup> We did not verify that the security enhancements reported to us by the water systems were actually taken. While we were in the process of determining which community water systems to select, three systems contacted us and volunteered to participate in our study. Because they met our criteria, we included these

---

<sup>2</sup>We interviewed operators of community water systems within the supply component of the water sector since critical infrastructure efforts within this sector have focused on community water systems.

<sup>3</sup>According to an EPA official, the smaller private systems are primarily owned and operated by a relatively few companies that also own and operate much larger private systems. Therefore, we focused on the larger systems to obtain an adequate perspective of privately held water systems.

<sup>4</sup>In January of 2005, we issued a report on experts' views regarding how federal funds should be spent to improve security. In this report, we stated that the vast majority of experts suggested that wastewater utilities serving critical infrastructure should be given the highest priority when allocating federal wastewater security funds. Furthermore, the activity that experts most frequently cited as deserving of federal funds to improve wastewater facilities security was the replacement of gaseous chemicals used in the disinfection process with less hazardous alternatives. See [GAO-05-165](#).



systems as part of our selection. We used a structured interview guide when questioning officials during our visits to these systems.

We are not disclosing the names or other identifying information relating to the individual chemical companies, facilities, or community water systems to ensure that security-related information is not unintentionally disclosed. Because we limited our review to 10 chemical facilities and 8 community water systems, the comments discussed in this report are illustrative, are not statistically representative of the chemical and water sectors, and should not be considered to represent the views of the sectors as a whole.

To determine the extent to which the chemical and water sectors' actions reflected a risk management approach, we reviewed provisions of the Responsible Care® Security Code, the Bioterrorism Act, and MTA that the chemical and water sectors are to follow. We then compared these provisions with elements of a risk management framework to determine which elements the sectors have incorporated and to identify those elements that were missing.<sup>5</sup>

To determine the results of the Coast Guard's compliance inspection program, we reviewed Coast Guard documents, such as inspection guidance, facility inspector checklists, and navigation and vessel information circulars regarding the procedures used to conduct the compliance inspections and the enforcement actions and operational controls available to the Coast Guard to address any deficiencies found during the inspection process. We also analyzed national compliance data provided by Coast Guard from its Marine Information for Safety and Law Enforcement (MISLE). To assess the reliability of these data, we examined the data for obvious errors and inconsistencies, reviewed existing documentation about their system and data, and examined responses the Coast Guard provided to a questionnaire we sent it requesting information on the administration and oversight of the system. We determined the

---

<sup>5</sup>GAO has consistently called for a risk management approach to homeland security issues. See GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, [GAO-02-208T](#) (Washington, D.C.: October 12, 2001); *Homeland Security: Key Elements of a Risk Management Approach*, [GAO-02-150T](#) (Washington, D.C.: Oct. 12, 2001); *Homeland Security: Summary of Challenges Faced in Targeting Ocean-going Cargo Containers for Inspection*, [GAO-04-557T](#) (Washington, D.C., Mar. 31, 2004); and *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, [GAO-04-598T](#) (Washington, D.C.: Mar. 23, 2004).

compliance data to be sufficiently reliable as general indicators of the results of the Coast Guard's inspection program.

To determine what actions the Coast Guard reported taking agencywide to ensure the effectiveness of the inspection program, we interviewed Coast Guard officials at headquarters with responsibilities for the compliance inspection process. To supplement this national-level perspective, we visited five local Coast Guard offices in locations that reflected diversity in strategic importance, geographic location, and local characteristics. The offices we visited were located in Charleston, South Carolina; Huntington, West Virginia; New Orleans, Louisiana; Houston, Texas; and Seattle, Washington. We conducted our work from October 2004 through March 2005 in accordance with generally accepted government auditing standards.

# Appendix II: Number of Community Water Systems

The Safe Drinking Water Information System is EPA's national database of public drinking water systems. Information from this system, presented in table 3, provides information on the number of community water systems in place during fiscal year 2004 by population service category and ownership.

**Table 3: Number of Community Water Systems by Ownership and Population Service Category for Fiscal Year 2004**

Ownership	Size of population served								All sizes
	100 or less	101-500	501-3,300	3,301-10,000	10,001-50,000	50,001-100,000	100,001-500,000	Over 500,000	
Private	11,484	9,995	3,480	569	331	66	43	9	25,977
Public	2,025	6,010	10,501	3,986	2,623	413	279	40	25,877
Unknown	257	235	231	152	103	5	0	1	984
<b>Total</b>	<b>13,766</b>	<b>16,240</b>	<b>14,212</b>	<b>4,707</b>	<b>3,057</b>	<b>484</b>	<b>322</b>	<b>50</b>	<b>52,838</b>

Source: U.S. Environmental Protection Agency's Safe Drinking Water Information System.

Note: The information in this chart is presented to provide context on the number of community water systems in the United States. GAO has not verified this data.

As reflected in the table, ownership of these systems is evenly split; about half are publicly owned and about half are privately owned. EPA does not have data on the ownership of approximately 2 percent, or 984, of these systems.

# Appendix III: Chemical Industry Trade Associations' Implementation of the Responsible Care® Security Code

The Responsible Care® Security Code calls for ACC's approximate 140 member companies to perform security vulnerability assessments of their approximately 2,000 facilities, develop and implement plans to mitigate the vulnerabilities, and obtain third-party verification that the planned physical security enhancements were completed. The Security Code sets milestones for facilities to complete these steps based on the level of potential impact a chemical release stemming from a facility would have on surrounding communities. ACC members assigned their facilities to "tiers" based on their assessment of this level of impact. A chemical release stemming from tier 1 facilities could have the greatest impact on surrounding communities, whereas a chemical release from tier 4 facilities would have no significant off-site impacts. The milestones for completion of these steps by each tier facility are depicted in table 4 below. ACC members operate approximately 100 tier 1 facilities, 350 tier 2 facilities, 550 tier 3 facilities, and 1,000 tier 4 facilities. Approximately 1,000 of ACC's facilities are among the 15,000 facilities—including, chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment.

**Table 4: Responsible Care® Security Code Deadlines for ACC Facilities**

<b>Actions required under the Responsible Care® Security Code</b>	<b>Tier 1</b>	<b>Tier 2</b>	<b>Tier 3</b>	<b>Tier 4</b>
Complete facility security vulnerability assessment	12/31/02	6/30/03	12/31/03	12/31/03
Complete implementation of facility security enhancements	12/31/03	6/30/04	12/31/04	12/31/04
Complete third-party verification of physical security enhancements	3/31/04	9/30/04	3/31/05	<sup>a</sup>

Source: American Chemistry Council.

<sup>a</sup>Because tier 4 facilities do not have potential significant off-site consequences, third-party verification is not required.

ACC reported that as of May 2004, all of its 2,000 facilities have completed security vulnerability assessments. ACC does not require its member companies to report the status of security enhancements until they report completion of third-party verification. ACC told us that based on the verification reports its members submitted, all tier 1 facilities have completed their security enhancements and their third-party verifications. Additionally, ACC told us that approximately 90 percent of its members, with tier 2 facilities have completed security enhancements and the enhancements have been verified. As of March 7, 2005, 10 percent of ACC

member companies are still working to complete their tier 2 verification requirements. ACC told us that it is in contact with these companies to provide any needed assistance, to monitor progress, and to ensure completion of these requirements as soon as possible.

SOCMA's 160 members also follow the provisions of the Responsible Care® Security Code. As members, they are expected to perform security vulnerability assessments of their facilities, develop and implement plans to mitigate the vulnerabilities found in the assessments, and obtain third-party verification that the planned physical security enhancements were completed. Thirty-six of SOCMA's member companies are also members of ACC and follow the Responsible Care® Security Code and related milestones as administered by ACC. The remaining 124 SOCMA companies are responsible for implementing the Responsible Care® Security Code under a SOCMA-established timetable as presented in table 5. These 124 companies operate 273 facilities—of which 77 are among the 15,000 facilities—including, chemical, water, energy, and other sector facilities—that produce, use, or store more than threshold amounts of chemicals that EPA has estimated pose the greatest risk to human health and the environment in the event of a release (risk management plan, or RMP, facilities).

**Table 5: Responsible Care® Security Code Deadlines for SOCMA Facilities**

<b>Actions required under the Responsible Care® Security Code</b>	<b>RMP facilities</b>	<b>Non-RMP facilities</b>
Complete facility security vulnerability assessment	6/30/03	12/31/03
Complete implementation of facility security enhancements	12/31/04	12/31/04
Complete verification of enhancements	3/31/05	<sup>a</sup>

Source: Synthetic Organic Chemical Manufacturers Association.

<sup>a</sup>Non-RMP facilities are not required to have third-party verification.

SOCMA officials told us that all of its member companies have reported completing vulnerability assessments at their 273 facilities. SOCMA also reports that 98 percent of these member companies reported completing implementation of security enhancements at their facilities.

---

# Appendix IV: Enforcement Actions Taken by the Coast Guard against MTSA-Regulated Facilities

---

The type of enforcement action the Coast Guard takes against maritime facilities for noncompliance with MTSA regulations depends on the type of deficiencies, the severity of the deficiencies, and the number of times a given facility has been cited for a deficiency. The enforcement actions taken by the Coast Guard against facility owners or operators include

- *Letter of warning:* A letter of warning is issued for deficiencies that can usually be immediately corrected but are severe enough to warrant documentation of noncompliance. A letter of warning can also be issued when the Coast Guard has previously informed a facility owner or operator of a less severe deficiency and the owner or operator has not yet addressed the deficiency upon a subsequent Coast Guard visit or spot check. Letters of warning document the deficiencies so that the Coast Guard has a case file in the event a more severe penalty is needed in the future to enforce compliance.
- *Notice of violation:* A notice of violation is issued when the deficiency requires additional investigation and a monetary penalty or when the Coast Guard has previously issued a letter of warning for the same deficiency but the facility owner or operator has not yet addressed the deficiency. With a notice of violation, the inspector issues a citation that provides the facility owner or operator immediate notification of the alleged violations and the penalty amount proposed by the Coast Guard. The owner or operator has the option of accepting the notice and paying the penalty amount or can decline the notice. If the owner or operator decides to decline, the case becomes a standard civil penalty (see below for explanation).
- *Civil penalty:* A civil penalty is used when a facility has several instances of noncompliance with the regulations. Typically initiated by a local Coast Guard unit, the civil penalty is submitted to the Coast Guard Hearing Office to determine if there is sufficient evidence to support the charges. Once the owner or operator has had an opportunity to respond to the charges, the Hearing Office issues its finding and the penalty, if any, is imposed on the owner or operator. The owner or operator may then appeal the decision to the Coast Guard Commandant.

The consequences are essentially the same for notices of violation as for standard civil penalty cases, because in both situations the Coast Guard assesses a civil penalty that becomes part of a facility owner or operator's violation history. The primary difference lies in the severity of the sanction, with the proposed penalty amounts for notices of violation generally lower than the recommended penalty levels for standard civil penalty cases. In addition, the Coast Guard will not issue a notice of

---

**Appendix IV: Enforcement Actions Taken by  
the Coast Guard against MTSA-Regulated  
Facilities**

---

violation for more than \$10,000, whereas the maximum civil penalty amount allowed by MTSA is \$25,000 for each violation, using the regular civil penalty process.

Table 6 shows the number of enforcement actions the Coast Guard reported taking against owners or operators of maritime facilities between July 1, 2004, and December 31, 2004, for noncompliance with MTSA regulations to implement their security plans. The specific regulatory cite topics in the table are listed in descending order of the total number of enforcement actions taken.

**Appendix IV: Enforcement Actions Taken by  
the Coast Guard against MTSA-Regulated  
Facilities**

**Table 6: Enforcement Actions Taken between July 1, 2004, and December 31, 2004, by Regulatory Citation Topic**

<b>Citation</b>	<b>Description of area of noncompliance</b>	<b>Number of enforcement actions taken</b>
33 CFR 105.255	Security measures for access control	89
33 CFR 105.200	Failure of facility owner or operator to ensure the facility operates in compliance with security requirements	38
33 CFR 105.205	Facility Security Officer requirements	34
33 CFR 105.260	Security measures for restricted areas	31
33 CFR 105.225	Failure of facility owner or operator to make the required records available to the Coast Guard	20
33 CFR 105.405	Failure to ensure proper format and content of the Facility Security Plan	13
33 CFR 105.210	Facility personnel with security duties	11
33 CFR 105.125	Failure of facility owner or operator to notify cognizant Captain of the Port of temporary deviations	9
33 CFR 105.275	Failure to implement security measures for monitoring as specified in the Facility Security Plan	9
33 CFR 105.265	Failure to implement security measures for handling cargo	8
33 CFR 105.245	Failure of a facility owner or operator to complete Declaration of Security	7
33 CFR 105.235	Failure to meet facility communications requirements	6
33 CFR 105.215	Security training for all other facility personnel	6
33 CFR 105.250	Failure to meet security systems and equipment maintenance requirements	5
33 CFR 105.270	Failure to implement security measures for delivery of vessel stores and bunkers	5
33 CFR 105.220	Failure of facility owner or operator to meet security drill requirements	4
33 CFR 105.285	Failure to meet additional requirements for passenger and ferry facilities	4
33 CFR 105.400	Failure to develop and implement a Facility Security Plan	4
33 CFR 105.120	Failure to provide compliance documentation	2
33 CFR 105.295	Failure to meet additional requirements for Certain Dangerous Cargo (CDC) facilities	2
33 CFR 105.140	Alternative Security Program	1
33 CFR 105.230	Maritime Security (MARSEC) Level coordination and implementation	1
33 CFR 105.240	Procedures for interfacing with vessels	1
33 CFR 105.290	Failure to meet additional requirements for cruise ship terminals	1
33 CFR 105.305	Failure of facility owner or operator to conduct a Facility Security Assessment	1
<b>Total</b>		<b>312</b>

Source: Coast Guard.



---

# Appendix V: Acknowledgments of Agency and Private Sector Contributors

---

We would like to acknowledge the time and effort made by federal agencies, trade associations, and security directors and other officials representing the chemical facilities, community water systems, and marine safety offices that provided information and talked with us during our site visits.

---

## Federal Agencies

Department of Homeland Security  
Environmental Protection Agency

---

## Trade Associations

American Chemistry Council  
Synthetic Organic Chemical Manufactures Association  
Association of Metropolitan Water Agencies  
National Association of Water Companies  
National Rural Water Association

# Appendix VI: Comments from the Department of Homeland Security

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



**Homeland  
Security**

March 16, 2005

Mr. William O. Jenkins  
Director, Homeland Security and Justice Issues  
Government Accountability Office  
Washington, DC 20548

Dear Mr. Jenkins:

Re: Draft Report GAO-05-327, Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges (GAO Job Code 440362)

Thank you for the opportunity to review your draft report. We concur with the purpose of the report and generally concur with its contents. Your report effectively discusses many of the regulatory and difficult financial challenges facing the chemical and water sectors in strengthening the security of their infrastructures.

Any such report can only represent a snapshot in time. In that context, it is understandable that the report does not fully reflect all the activities currently ongoing in this area. For example, the report does not mention the efforts currently underway to improve government and private sector infrastructure protection coordination efforts through the formation of Government Coordinating Councils and Sector Coordinating Councils. The report also notes that GAO did not have time to fully evaluate the Interim National Infrastructure Protection Plan (NIPP). DHS agrees that a rigorous risk management approach is central to an effective infrastructure protection program and believes that the NIPP lays out an effective risk management framework. These observations do not alter our view that the report presents generally valuable and useful information.

A technical comment will be sent under separate cover. We thank you again for the opportunity to review the report and provide comments.

Sincerely,

A handwritten signature in black ink that reads "Steven J. Pecinovsky".

Steven J. Pecinovsky  
Acting Director,  
Departmental GAO/OIG Liaison Office

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

---

# Appendix VII: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

William O. Jenkins, Jr. (202) 512-8777  
Debra B. Sebastian (202) 512-9385

---

## Acknowledgments

In addition to the individuals named above, David P. Alexander, Jonathan T. Bachman, Fredrick D. Berry, Beatriz Cuartas, Grace A. Coleman, Dorian R. Dunbar, Michele C. Fejfar, Geoffrey R. Hamilton, Christopher Hatscher, Sara R. Margraf, and Diane B. Raynes made key contributions to this report.

---

# Related GAO Products

---

*High-Risk Series: An Update.* [GAO-05-207](#). Washington, D.C. January 1, 2005.

*Wastewater Facilities: Experts' Views on How Future Federal Funds Should Be Spent to Improve Security.* [GAO-05-165](#). Washington, D.C.: January 31, 2005.

*Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security.* [GAO-05-33](#). Washington, D.C.: January 14, 2005.

*Drinking Water: Experts' Views on How Federal Funding Can Best Be Spent to Improve Security.* [GAO-04-1098T](#). Washington, D.C.: September 30, 2004.

*Public Key Infrastructure: Examples of Risks and Internal Control Objectives Associated with Certification Authorities.* [GAO-04-1023R](#). Washington, D.C.: August 10, 2004.

*Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security.* [GAO-04-838](#). Washington, D.C.: June 30, 2004.

*Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors.* [GAO-04-780](#). Washington, D.C.: July 9, 2004.

*Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors.* [GAO-04-699T](#). Washington, D.C.: April 21, 2004.

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* [GAO-04-628T](#). Washington, D.C.: March 30, 2004.

*Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain.* [GAO-04-598T](#). Washington, D.C.: March 23, 2004.

*Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection.* [GAO-04-557T](#). Washington, D.C.: March 31, 2004.

*Homeland Security: Federal Action Needed to Address Security Challenges at Chemical Facilities.* [GAO-04-482T](#). Washington, D.C.: February 23, 2004.

*Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems.* [GAO-04-354](#). Washington, D.C.: March 15, 2004.

*Technology Assessment: Cybersecurity for Critical Infrastructure Protection.* [GAO-04-321](#). Washington, D.C.: May 28, 2004.

*Terrorism Insurance: Implementation of the Terrorism Risk Insurance Act of 2002.* [GAO-04-307](#). Washington, D.C.: April 23, 2004.

*Posthearing Questions from the September 17, 2003, Hearing on Implications of Power Blackouts for the Nation's Cybersecurity and Critical Infrastructure Protection: The Electric Grid, Critical Interdependencies, Vulnerabilities, and Readiness.* [GAO-04-300R](#). Washington, D.C.: December 8, 2003.

*Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security.* [GAO-04-29](#). Washington, D.C.: October 31, 2003.

*Critical Infrastructure Protection: Challenges in Securing Control Systems.* [GAO-04-140T](#). Washington, D.C.: October 1, 2003.

*Information Security: Progress Made, but Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures.* [GAO-03-564T](#). Washington, D.C.: April 8, 2003.

*Homeland Security: EPA's Management of Clean Air Act Chemical Facility Data.* [GAO-03-509R](#). Washington, D.C.: March 14, 2003.

*Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments.* [GAO-03-502](#). Washington, D.C.: May 1, 2003.

*Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown.* [GAO-03-439](#). Washington, D.C.: March 14, 2003.

*Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors.* [GAO-03-233](#). Washington, D.C.: February 28, 2003.

*Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats.* [GAO-03-173](#). Washington, D.C.: January 30, 2003.

*High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures.* [GAO-03-121](#). Washington, D.C.: January 1, 2003.

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

*Critical Infrastructure Protection: Significant Challenges Need to Be Addressed.* [GAO-02-961T](#). Washington, D.C.: July 24, 2002.

*Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed.* [GAO-02-918T](#). Washington, D.C.: July 9, 2002.

*Chemical Safety: Emergency Response Community Views on the Adequacy of Federally Required Chemical Information.* [GAO-02-799](#). Washington, D.C.: July 31, 2002.

*Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems.* [GAO-02-474](#). Washington, D.C.: July 15, 2002.

*Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts,* [GAO-02-208T](#). Washington, D.C.: October 31, 2001.

*Key Elements of a Risk Management Approach.* [GAO-02-150T](#). Washington, D.C.: Oct. 12, 2001.

*Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks.* [GAO-01-1168T](#). Washington, D.C.: September 26, 2001.

---

## 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