United States Government Accountability Office

GAO

Testimony

Before the Committee on Environment and Public Works, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, June 21, 2006

HOMELAND SECURITY

DHS Is Addressing Security at Chemical Facilities, but Additional Authority Is Needed

Statement for the Record by
John B. Stephenson, Director
Natural Resources and Environment

June 21, 2006

HOMELAND SECURITY

DHS Is Addressing Security at Chemical Facilities, but Additional Authority Is Needed

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-899T, testimony before the Senate Committee on Environment and Public Works

Why GAO Did This Study

Terrorist attacks on U.S. chemical facilities could damage public health and the economy. The Department of Homeland Security (DHS) coordinates federal efforts to protect these facilities from attacks.

GAO was asked to provide a statement for the record based on its report *Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed* (GAO-06-150, January 27, 2006), GAO reviewed (1) DHS's actions to develop a strategy to protect chemical plants, assist with the industry's security efforts, and coordinate with other federal agencies, (2) industry security initiatives, (3) DHS's authorities and the need for additional security legislation, and (4) stakeholders' views on any requirements to use safer technologies.

What GAO Recommends

GAO's report recommended that (1) the Congress consider giving DHS the authority to require the chemical industry to address plant security, (2) DHS complete its Chemical Sector-Specific Plan in a timely manner, and (3) DHS study, with the Environmental Protection Agency (EPA), the security benefits of using safer technologies. DHS agreed in substance with GAO's first two recommendations but expressed concerns about studying safer technologies. GAO continues to see merit in such a study. EPA had no comments on the report.

www.gao.gov/cgi-bin/getrpt?GAO-06-899T.

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

What GAO Found

DHS is developing a Chemical Sector-Specific Plan, which is intended to, among other things, describe DHS's ongoing efforts and future plans to coordinate with federal, state, and local agencies and the private sector; identify chemical facilities to include in the sector, assess their vulnerabilities, and prioritize them; and develop programs to prevent, deter, mitigate, and recover from attacks on chemical facilities. DHS officials told GAO that they now expect to complete and release the plan in the fall of 2006. In addition, DHS has taken a number of actions to protect the chemical sector from terrorist attacks. DHS identified 3,400 facilities that, if attacked, could pose the greatest hazard to human life and health and has initiated programs to assist the industry and local communities in protecting chemical plants. DHS also coordinates with the Chemical Sector Coordinating Council, an industry-led group that acts as a liaison for the chemical sector, and with EPA and other federal agencies.

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

Because existing laws provide DHS with only limited authority to address security at chemical facilities, it has relied primarily on the industry's voluntary security efforts. However, the extent to which companies are addressing security is unclear. DHS does not have the authority to require chemical facilities to assess their vulnerabilities and implement security measures. Therefore, DHS cannot ensure that facilities are taking these actions. DHS has stated that its existing authorities do not permit it to effectively regulate the chemical industry, and that the Congress should enact federal requirements for chemical facilities. Many stakeholders agreed—as GAO concluded in 2003 and again in January 2006—that additional legislation placing federal security requirements on chemical facilities is needed.

Stakeholders had mixed views on whether any chemical security legislation should require plants to substitute safer chemicals and processes, which could lessen the potential consequences of an attack, but could be costly or infeasible for some plants. DHS has stated that safer practices may make facilities less attractive to terrorist attack, but may shift risks rather than eliminate them. Environmental groups told GAO that they favored including or considering inherently safer technologies in any federal requirements, but most industry officials GAO contacted opposed a requirement to use safer technologies because they may shift risks or be prohibitively expensive.

Mr. Chairman and Members of the Committee:

We are pleased to have the opportunity to present the results of our recent work on chemical facility security.[1] As we reported in January 2006, across the nation, approximately 15,000 facilities produce, use, or store more than specific maximum amounts of chemicals that the Environmental Protection Agency (EPA) has identified as posing the greatest risk to human health and the environment if accidentally released into the air. These facilities include chemical manufacturers, storage and distribution facilities, water and wastewater treatment facilities, and refineries, among others. Since September 11, 2001, government and other experts have recognized the potential threat that chemical facilities pose because many house toxic chemicals that could become airborne and drift to surrounding areas or be used to create a chemical weapon capable of causing harm. While these facilities potentially put large numbers of Americans at risk of injury or death in the event of a chemical release, the chemicals they produce, use, store, and distribute are critical to the nation's economy.

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) and set forth its mission to, among other things, prevent terrorist attacks in the United States and reduce the vulnerability of the nation to terrorism.[2] The President's February 2003 National Strategy for the Physical Protection of Critical Infrastructures and Key Assets sets forth the federal government's roles, objectives, and responsibilities in protecting the nation's critical infrastructure, including the chemical industry. In addition, a December 2003 presidential directive instructed DHS to produce a comprehensive integrated plan outlining national goals, objectives, milestones, and key initiatives for protecting critical infrastructure and key resources.[3] The directive also named DHS as the lead agency for the chemical sector. [4] Under an interim national plan released in February 2005, DHS is to identify and prioritize critical

[1]GAO, Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed, GAO-06-150 (Washington, D.C.: January 27, 2006).

[2]Pub. L. No. 107-296, § 101(b), 116 Stat. 2135, 2142 (2002).

[3]Homeland Security Presidential Directive Number 7, section 27 (Washington, D.C.: Dec. 17, 2003).

[4]Homeland Security Presidential Directive Number 7, section 15 (Washington, D.C.: Dec. 17, 2003).

chemical facilities, evaluate the chemical sector's vulnerabilities and risks, develop and implement protective programs for high-priority chemical facilities, identify regulatory options for protective measures, and maintain a relationship with all stakeholders.

The federal government's role in protecting chemical facilities from terrorist attacks has been much debated since September 11, 2001. Public debate has centered on whether the federal government should impose security requirements on chemical facilities or continue to work with the chemical industry to voluntarily address security concerns. Legislative proposals that would grant DHS or EPA, or one of these agencies in consultation with the other, the authority to require chemical facilities to take security steps were introduced in every Congress from 2001 to 2005. Provisions in legislative proposals that would require chemical facilities to implement or consider the substitution of safer chemicals and processes—referred to as "inherently safer technologies"—have also sparked debate. Appendix I provides an overview of key chemical security legislative proposals in the 109th Congress, two of which contain provisions relating to the use of inherently safer technologies.

My statement today is based on our January 2006 report, and will focus on (1) DHS' actions to develop a plan for protecting the chemical sector, assess facilities' vulnerabilities, and interact with the industry and other federal agencies; (2) chemical industry security initiatives and challenges; (3) DHS' existing authorities and whether additional legislative authority is needed; and (4) stakeholders' views on the inclusion of an inherently safer technologies requirement in any legislation. In conducting our work, we interviewed officials from DHS and EPA and reviewed pertinent federal legislation, EPA data, DHS documents, and other available reports. We also interviewed representatives of all 16 associations participating on the Chemical Sector Coordinating Council, a group of chemical sector associations that facilitate the sharing of industry views with DHS, and spoke with at least one member company belonging to 13 of the key

chemical industry associations.[5] We also interviewed other organizations with chemical industry expertise, including the American Society of Mechanical Engineers, the Center for Chemical Process Safety, Sandia National Laboratories, and the Working Group on Community Right-to-Know, among others. We conducted our work according to generally accepted government auditing standards.

Summary

In summary, we found the following:

- As of January 2006, when we issued our report, DHS was developing a Chemical Sector-Specific Plan as part of a national framework to reduce the overall vulnerability of the chemical sector. According to DHS, the plan will describe, among other things, the chemical industry; DHS' coordination with federal, state, and local agencies and with the private sector; DHS' efforts to identify and prioritize chemical facilities on the basis of risk; and DHS' development of protective programs to prevent, deter, mitigate, and recover from attacks on chemical facilities. In developing this plan, DHS initiated actions to identify the sector's critical assets, prioritize facilities, develop and implement programs, exchange information with the private sector, and coordinate efforts with EPA and other federal agencies. For example, DHS identified about 3,400 high-priority facilities and plans to use a new risk assessment methodology to compare and prioritize all critical infrastructure assets according to their level of threat, vulnerability to attack, and the consequences of an attack. DHS officials told us that they expect to complete and release the sector-specific plan in the fall of 2006.

- The chemical industry, led by its industry associations, has undertaken voluntary efforts to address plant security, but faces challenges in preparing facilities against terrorism. Some industry associations require their member companies to assess facilities' vulnerabilities and make

[5]As of November 2005, Chemical Sector Coordinating Council members included the Adhesive and Sealant Council; the American Chemistry Council; the American Forest & Paper Association; the Chemical Producers and Distributors Association; the Chlorine Chemistry Council; the Chlorine Institute; the Compressed Gas Association; CropLife America; the Fertilizer Institute; the Institute of Makers of Explosives; the International Institute of Ammonia Refrigeration; the National Association of Chemical Distributors; the National Paint and Coatings Association; the National Petrochemical and Refiners Association; the Society of the Plastics Industry, Inc.; and the Synthetic Organic Chemical Manufacturers Association. Three associations—the Adhesive and Sealant Council, the International Institute of Ammonia Refrigeration, and the National Paint and Coatings Association—were not able to identify a member company willing to speak with us.

security enhancements. For example, the American Chemistry Council, a chemical industry association, requires as a condition of membership that companies conduct vulnerability assessments, develop and implement plans to mitigate vulnerabilities, and have a third party verify that the security enhancements were implemented. The Council reports that its members have spent an estimated $2 billion on security improvements since September 11, 2001. Other industry associations have developed security guidelines, best practices, and other tools and a number of associations have developed security guidelines and vulnerability assessment methodologies tailored specifically to their member companies' unique security concerns. However, industry officials told us that they face a number of challenges in preparing facilities against a terrorist attack. They reported that the cost of security improvements can be a burden, particularly for smaller companies, and that determining the appropriate level of security for different facilities is difficult without guidance on what level of security is adequate.

- Existing laws provide DHS with only limited authority to address security concerns at U.S. chemical facilities. To require security improvements at these facilities, which pose significant risks to millions of Americans, DHS needs additional legislative authority. DHS lacks the authority to require chemical facilities to assess their vulnerabilities and implement security measures and cannot enter most chemical facilities without their permission to assess security or to enforce the implementation of any needed security improvements. In contrast to some other critical infrastructure facilities—such as nuclear and drinking water facilities—chemical plants generally are not subject to federal security requirements. Consequently, DHS has relied primarily on the private sector's voluntary participation to address facility security. As a result, DHS cannot ensure that all high-risk facilities are assessing their vulnerability to terrorist attacks and taking corrective actions, where necessary. On this basis, we concluded in 2003 and again in January 2006 that additional legislation is needed to place federal security requirements on chemical facilities.[6] In addition, DHS has concluded that its existing authorities do not permit it to effectively regulate the industry, and that the Congress should enact federal requirements for chemical facilities. Given that the nation's chemical facilities pose significant risks and the extent of their security preparedness is largely unknown, legislation giving DHS the authority to

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

require the chemical industry to address security at their plants is long overdue.

- While many of the stakeholders we contacted—including representatives from industry, research centers, and government—agreed on the need for additional legislation establishing federal security requirements, they had divergent views on whether facilities should be required to use safer chemicals and processes—referred to as "inherently safer technologies." Inherently safer technologies could lessen the potential consequences of an attack by reducing the risks present at these facilities, but could be costly or infeasible for some plants. The Department of Justice and DHS have recognized that safer practices, such as reducing the quantity of hazardous material on site may make facilities less attractive to terrorist attack or could prevent or delay a terrorist attack. However, DHS officials told us that the use of inherently safer technologies tends to shift risks rather than eliminate them, often with unintended consequences. Representatives from environmental groups, as well as process safety experts, told us that the inherently safer technologies should be included or considered in any federal chemical security requirements. In contrast, the majority of the industry officials we contacted opposed a requirement to use inherently safer technologies because their use may shift risks or be prohibitively expensive.

To ensure that chemical facilities take action to review and address security vulnerabilities, we recommended in January 2006 that

- the Congress consider providing DHS with the authority to require high-risk chemical facilities to assess their vulnerability to terrorist attacks and, where necessary, require these facilities to take corrective action, and

- DHS complete the Chemical Sector-Specific Plan in a timely manner and work with EPA to study the advantages and disadvantages of substituting safer chemicals and processes at some chemical facilities.

In comments responding to a draft of our January 2006 report, DHS agreed that the Congress should consider granting DHS the authority to require the chemical industry to address plant security and that completing and implementing the sector-specific plan is a priority. Legislation is before the Congress that, if enacted, would direct DHS to require high-risk chemical facilities to assess their vulnerability to terrorist attacks and take corrective action, where necessary. Furthermore, DHS officials expect to complete and release the sector-specific plan in the fall of 2006. However, DHS disagreed with our recommendation that the department work with EPA to study the security benefits of using safer technologies. As noted,

DHS believes that the use of safer technologies would not generally result in more secure chemical facilities and would shift risks rather than eliminate them. DHS also stated that it is unclear what role EPA would play in a study of the benefits of using safer technologies or how DHS's interaction with EPA might be perceived among DHS's private sector partners.

We continue to believe, however, that the use of safer technologies may have the potential to reduce security risks for at least some chemical facilities by making them less attractive to a terrorist attack and reducing the severity of the potential consequences of an attack and that studying the costs and security benefits of using safer technologies would be a worthwhile effort. While DHS should have the lead role in conducting such a study, EPA can provide valuable support. EPA has extensive expertise on toxic chemical data sources, U.S. hazardous materials facilities, and process safety issues, among other things, that the agency has developed through its oversight of a number of chemical safety programs. In particular, EPA maintains data on high-risk facilities' inventories of toxic and flammable chemicals and facility worst-case release scenarios, which could be useful to DHS in studying inherently safer technologies. Furthermore, we do not believe that a DHS-EPA partnership to study safer chemicals and technologies would necessarily bring the department into conflict with the industry, if the appropriate informational safeguards and assurances are built into the process. Through additional study, these two agencies can help to determine the appropriate role of inherently safer technologies in government and industry efforts to bolster chemical facility security and could identify alternative ways to reduce security, environmental, and health risks that could be shared with private industry.

Background

Experts agree that chemical facilities are among the most attractive targets for terrorists intent on causing massive damage. Despite the risk these facilities pose, no one has yet comprehensively assessed security at the nation's chemical facilities. EPA regulates about 15,000 facilities under the 1990 amendments to the Clean Air Act because they produce, use, or store more than certain threshold amounts of specific chemicals that would pose the greatest risk to human health and the environment if they were accidentally released into the air. These facilities must take a number of steps, including preparing a risk management plan (RMP), to prevent and prepare for an accidental release and, therefore, are referred to as RMP facilities. These facilities fall within a variety of industries and produce, use, or store a variety of products, including basic chemicals; specialty chemicals, such as solvents; life science chemicals, such as

pharmaceuticals and pesticides; and consumer products, such as cosmetics. Some of these facilities are part of critical infrastructure sectors other than the chemical sector. For example, about 2,000 of these facilities are community water systems that are part of the water infrastructure sector. In addition, other facilities that house hazardous chemicals that are listed under the RMP regulations are not subject to RMP requirements because the quantities stored or used are below threshold amounts. Through the RMP program, EPA has gained extensive expertise with chemical facilities and processes that could be useful in helping DHS assess security issues.

Federal requirements currently address security at some U.S. chemical facilities. For example, a small number of chemical facilities must comply with the Maritime Transportation Security Act of 2002 and its implementing regulations, which require maritime facility owners and operators to conduct assessments, develop security plans, and implement security measures. In addition, certain community water systems—while not specifically considered chemical facilities but which use and store large volumes of chemicals—are required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 to conduct and submit a vulnerability assessment to EPA and prepare an emergency response plan that incorporates the results of the assessment. According to EPA, 1,928 drinking water facilities that are also subject to EPA's RMP program must comply with this act. Some states and localities have also created security requirements at chemical facilities.

In addition, the federal government imposes safety and emergency response requirements on chemical facilities that may incidentally reduce the likelihood and consequences of terrorist attacks. For example, Section 112(r) of the Clean Air Act includes a general duty clause directing owners and operators of facilities to identify hazards, design and maintain a safe facility to prevent releases, and minimize the consequences of any accidental releases that occur. [7] Under Section 112(r), RMP facilities must also implement a program to prevent accidental releases that includes safety precautions and maintenance, and monitoring and training measures, and they must have an emergency response plan. The Department of Labor's Occupational Safety and Health Administration's process safety management standard also requires facilities to conduct analyses of their chemical processes which must address hazards of the

[7]See 42 U.S.C. § 7412 (r)(1).

process, engineering and administrative controls applicable to the hazards, facilities siting, and evaluation of the possible health and safety effects of failures of controls on employees.

DHS Has Taken Actions to Develop a Plan for Protecting the Chemical Sector, Assess Facilities' Vulnerabilities, and Interact with the Industry and Other Federal Agencies

DHS is developing a plan for protecting the chemical sector that will establish a framework for reducing the overall vulnerability of the sector in partnership with the industry and state and local authorities. At the time of our review, DHS did not provide a specific date for completion of the Chemical Sector-Specific Plan. DHS completed a draft of the plan in July 2004 and has been working to revise it to accommodate changes to DHS's risk management strategy and comments from stakeholders. DHS officials told us that the final plan—which they now expect to complete and release in the fall of 2006—will reflect the basic principles and content described in the draft plan. On the basis of our review of the draft plan and discussions with DHS officials, the final plan will, among other things, (1) present background information on the sector; (2) describe the process DHS will use to develop an inventory of chemical sector assets; (3) describe DHS's efforts to identify and assess chemical facilities' vulnerabilities and plans to prioritize these efforts on the basis of the vulnerability assessments; (4) outline the protective programs that will be created to prevent, deter, mitigate, and recover from attacks on chemical facilities, and describe how DHS will work with private sector and government entities to implement these programs; (5) explain the performance metrics DHS will use to measure the effectiveness of DHS and industry security efforts; and (6) outline the department's challenges in coordinating the efforts of the chemical sector.[8]

DHS has also initiated actions to identify the chemical sector's critical assets, prioritize facilities, develop and implement protective programs, exchange information with the private sector, and coordinate efforts with EPA and other federal agencies. DHS is focusing its efforts for the chemical sector by identifying high-priority facilities. As a starting point, DHS has adapted EPA's RMP database of facilities with more than

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

threshold amounts of certain chemicals to develop an interim inventory of 3,400 chemical facilities that pose the greatest hazard to human life and health in the event of a terrorist attack. These are facilities where a worst-case scenario release potentially could affect over 1,000 people. According to DHS, 272 of these facilities could potentially affect more than 50,000 people.

DHS is also developing a new risk assessment methodology to compare and prioritize all critical infrastructure assets according to their level of threat, their vulnerability to attack, and the consequences of an attack on the facility. According to DHS, Risk Analysis Management for Critical Asset Protection (RAMCAP) will provide a common methodology, terminology, and framework for homeland security risk analysis and decision making that is intended to allow consistent risk management across all sectors. The RAMCAP process entails chemical facility owners/operators voluntarily completing a screening tool to identify the consequences of an attack. On the basis of the results of the screening tool, DHS will identify facilities of highest concern and ask them to voluntarily complete a security vulnerability assessment.

Finally, DHS has implemented a number of programs to assist the private sector and local communities in reducing vulnerabilities. For example, DHS works with local law enforcement officials and facility owners through the Buffer Zone Protection Program to improve the security of the area surrounding a facility. To assess and identify vulnerabilities at chemical facilities, DHS deploys teams of experts from both government and industry to conduct a site assistance visit. DHS had conducted 38 site assistance visits at chemical facilities as of June 15, 2005, and planned to conduct additional visits in fiscal year 2006 on the basis of need. DHS has also installed cameras at some high-consequence facilities, providing local law enforcement authorities with the ability to conduct remote surveillance and allowing state homeland security offices and DHS to monitor the facilities. In addition, DHS distributes threat information to the industry through various means and coordinates sector activities with the Chemical Sector Coordinating Council, an industry-led working group formed voluntarily by trade associations that acts as a liaison for the chemical sector. DHS also coordinates with EPA and other federal agencies through a government coordinating council. EPA officials believe that the agency could further assist DHS by providing analytical support in identifying high-risk facilities that should be targeted in DHS' chemical sector efforts, among other activities.

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

With few federal security requirements, industry associations have been active in promoting security among member companies. Some industry associations, including the American Chemistry Council (ACC), the Synthetic Organic Chemical Manufacturers Association, and the National Association of Chemical Distributors, require member companies to assess their facilities' vulnerabilities and make security enhancements, requiring as a condition of membership that they conduct security activities and verify that these actions have been taken. ACC, representing 135 chemical manufacturing companies with approximately 2,000 facilities, has led the industry's efforts to improve security at their facilities. ACC requires its members to adhere to a set of security management principles that include performing physical security vulnerability assessments using an approved methodology, developing plans to mitigate vulnerabilities, taking actions to implement the plans, and having an independent party such as insurance representatives or local law enforcement officials verify that the facilities implemented the identified physical security enhancements. These reviewers do not verify that a vulnerability assessment was conducted appropriately or that actions taken by a facility adequately address security risks. However, ACC requires member companies to periodically conduct independent third-party audits that include an assessment of their security programs and processes and their implementation of corrective actions. In addition, ACC members must take steps to secure cyber assets, such as computer systems that control chemical facility operations, and the distribution chain from suppliers to customers, including transportation.

Other industry associations have encouraged their members to address security by a variety of means. Most of the 16 associations we spoke to have developed security guidelines and best practices. For example, the International Institute of Ammonia Refrigeration, representing facilities such as food storage warehouses, developed site security guidelines tailored to ammonia refrigeration facilities and provides information about security resources to members. Several industry associations have also developed vulnerability assessment methodologies to assist their member companies in evaluating security needs. For example, the National Petrochemical and Refiners Association, in partnership with the American Petroleum Institute, developed a vulnerability assessment methodology tailored to refiners and petrochemical facilities. Despite industry associations' efforts to encourage or require members to voluntarily address security, the extent of participation in the industry's voluntary initiatives is unclear.

Chemical industry officials told us they face a number of challenges in preparing facilities against a terrorist attack. Most of the chemical associations we contacted stated that the cost of security improvements is a challenge for some chemical companies. For example, ACC reports that its members have spent an estimated $2 billion on security improvements since September 11, 2001. Representatives of the American Forest & Paper Association and the National Paint and Coatings Association told us that small companies, in particular, may struggle with the cost of security improvements or the cost of complying with any potential government security programs because they may lack the resources larger companies have to devote to security. Industry stakeholders also cited the need for guidance on what level of security is adequate. While DHS has issued guidance to state Homeland Security Offices and the Chemical Sector Coordinating Council on vulnerabilities and protective measures that are common to most chemical facilities, several stakeholders expressed a desire for guidance on specific security improvements. For example, representatives of the National Petrochemical and Refiners Association stated that one reason the association holds workshops and best practices sessions is to meet the challenge of determining the types of security measures that constitute a reasonable amount of security.

In addition, industry officials told us that the lack of threat information makes it difficult for companies to know how to protect facilities. A few industry officials also mentioned limited guidance on conducting vulnerability assessments and difficulty in conducting employee background checks as challenges. One industry association stated that it would like its members to receive guidance from DHS on how to conduct vulnerability assessments. Another association expressed frustration because none of the current vulnerability assessment tools address issues specific to their member facilities, which package and distribute chemicals, and it would like DHS to help develop or approve a methodology for this type of facility. Finally, a number of stakeholders we contacted told us that emergency response preparedness is a challenge for chemical companies. An official with an industry-affiliated research center asserted that emergency responders and communities in the United States are prepared to respond to a toxic release. However, other stakeholders we spoke with stated that many facilities have conducted security vulnerability assessments but may not have done enough emergency response planning and outreach to the responders and communities that would be involved in a release. A 2004 survey by a chemical workers union of workers at 189 RMP facilities found that only 38 percent of respondents indicated that their companies' actions in preparing to respond to a terrorist attack were effective, and 28 percent reported that no employees

at their facilities had received training about responding to a terrorist attack since September 11, 2001.[9] While environmental laws require emergency response planning for accidental chemical releases, several stakeholders told us facilities need to consider very different scenarios with consequences on different orders of magnitude when planning the emergency response for a terrorist incident.

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

Existing laws give DHS limited authority to address chemical sector security, but DHS currently lacks specific authority to require all high-risk facilities to assess their vulnerabilities and take corrective actions, where needed. A number of existing laws outline DHS's responsibilities for coordinating with the private sector and obtaining information on and protecting critical infrastructure, but these laws provide DHS with only limited authority to address security concerns at U.S. chemical facilities. For example, under the Homeland Security Act, the Secretary of DHS is responsible for coordinating homeland security issues with the private sector to ensure adequate planning, equipment, training, and exercise activities.[10] Furthermore, the Act gives DHS's Under Secretary for Information Analysis and Infrastructure Protection (IAIP) responsibilities related to protecting critical infrastructure, including

- accessing, receiving, analyzing, and integrating information from federal, state, and local governments and private sector entities to identify, detect, and assess the nature and scope of terrorist threats to the United States;
- carrying out comprehensive assessments of the vulnerabilities of the nation's key resources and critical infrastructure;
- developing a comprehensive national plan for securing the nation's key resources and critical infrastructure; and

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

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

- recommending the necessary measures to protect these key resources and critical infrastructure.

DHS does not currently have the authority to require all chemical facilities to conduct vulnerability assessments or to enter chemical facilities without their permission to assess security or to require and enforce security improvements.[11] There is also no legislation requiring chemical facilities to provide information about their security and vulnerabilities. Furthermore, except with respect to certain chemical facilities covered under federal security requirements for other critical infrastructures, existing laws do not give DHS the right to enter a chemical facility to assess its vulnerability to a terrorist attack or the authority to require and enforce the implementation of any needed security improvements at these facilities. The Homeland Security Act, with some limited exceptions, does not provide any new regulatory authority to DHS and only transferred the existing regulatory authority of any agency, program, or function transferred to DHS, thereby limiting actions DHS might otherwise be able to take under the Homeland Security Act.[12] Therefore, DHS has relied solely on the voluntary participation of the private sector to address facility security. As a result, DHS cannot ensure that all high-risk facilities are assessing their vulnerability to terrorist attacks and taking corrective action, where necessary.

DHS has concluded that its existing patchwork of authorities does not permit it to regulate the chemical industry effectively, and that the Congress should enact federal requirements for chemical facilities. Echoing public statements by the Secretary of Homeland Security and the Administrator of EPA in 2002 that voluntary efforts alone are not sufficient to assure the public of the industry's preparedness, in June 2005, both DHS and EPA called for legislation to give the federal government greater

[11]Under the Maritime Transportation Security Act, DHS's Coast Guard requires maritime facility owners/operators to conduct assessments of vulnerabilities, develop security plans, and implement security measures. The Coast Guard also has the authority to enter facilities. However, the Coast Guard reports that these requirements currently apply to only 300 chemical facilities.

[12]The Secretary may issue regulations for antiterrorism technology and may issue necessary regulations with respect to research; development; demonstration; testing; and evaluation activities of the department, including the conducting, reviewing, and funding of such activities.

authority over chemical facility security.[13] Similarly, we concluded in 2003, and continue to believe, that additional federal legislation is needed because of the significant risks posed by thousands of chemical facilities across the country to millions of Americans and because the extent of security preparedness at these facilities is unknown.[14]

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

Stakeholders' Views on Safer Technologies Requirement in Chemical Security Legislation Are Mixed

While many stakeholders—including representatives from industry, research centers, and government—agreed on the need for additional legislation that would place federal security requirements on chemical facilities, they expressed divergent views on whether such legislation should require the use of inherently safer technologies. Implementing inherently safer technologies could potentially lessen the consequences of an attack by reducing the chemical risks present at facilities. The Department of Justice, in introducing a methodology to assess chemical facilities' vulnerabilities, recognized that reducing the quantity of hazardous material may make facilities less attractive to terrorist attack and reduce the severity of an attack. Furthermore, DHS's July 2004 draft Chemical Sector-Specific Plan states that inherently safer chemistry and engineering practices can prevent or delay a terrorist incident, noting that

[13]Testimony before the House Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity and the Senate Committee on Homeland Security and Governmental Affairs on June 15, 2005.

[14]GAO-03-439.

it is important to make sure that facility owners/operators consider alternate ways to reduce risk, such as using inherently safer design, implementing just-in-time manufacturing, or replacing high-risk chemicals with safer alternatives. However, DHS told us that the use of inherently safer technologies tends to shift risks rather than eliminate risks, often with unintended consequences. Some previous chemical security legislative proposals have included a requirement that facility security plans include safer design and maintenance actions, or that facility security plans include "consideration" of alternative approaches regarding safer design.

Representatives from three environmental groups told us that facilities have defined security too narrowly, without focusing on reducing facility risks through safer technologies. Noting that no existing laws require facilities to analyze inherently safer options, these representatives believe legislation should require such an analysis and give DHS or EPA the authority to require the implementation of technologies if high-risk facilities are not doing so. Process safety experts at one research organization recognized that reducing facility hazards and the potential consequences of chemical releases makes facilities less vulnerable to attack. However, these experts also explained that inherently safer technologies can be prohibitively expensive and can shift risks onto other facilities or the transportation sector. For example, reducing the amount of chemicals stored at a facility may increase reliance on rail or truck shipments of chemicals. However, the substitution of chemicals such as liquid bleach for chlorine gas at drinking water facilities reduces overall risks. These experts support legislative provisions requiring analysis or consideration of technology options but do not support giving the federal government the authority to require specific technology changes because of the complexity of these decisions. Representatives of two research centers affiliated with the industry told us that while facilities should look at inherently safer technologies when assessing their vulnerability to terrorist attack, safer technologies are not a substitute for security.

Industry associations and company officials were strongly opposed to any requirements to use inherently safer technologies. The majority of the industry officials we contacted opposed an inherently safer technologies requirement, with many stating that inherently safer technologies involve a safety issue that is unrelated to facility security. Industry officials voiced concerns about the federal government's second-guessing complex safety decisions made by facility process safety engineers. Representatives from four associations and two companies told us that, in many cases, it is not feasible to substitute safer chemicals or change to safer processes. Certain

hazardous chemicals may be essential to necessary chemical processes, while changing chemical processes may require new chemicals that carry different risks. In July 2005 testimony before the Congress, a Synthetic Organic Chemical Manufacturers Association representative explained that while inherently safer technologies are intended to reduce the overall risks at a facility, they could do so only if a chemical hazard was not displaced to another time or location or did not magnify another hazard. Furthermore, process safety experts and representatives from associations and companies report that some safer alternatives are extremely expensive. For example, reducing facility chemical inventories by moving to on-site manufacturing when chemicals are needed can cost millions of dollars, according to a stakeholder. One company also voiced opposition even to a legislative requirement that facilities "consider" safer options. The official explained that the company opposed such a provision—even if legislation does not explicitly give the government the authority to require implementation of safer technologies—because it might leave companies liable for an accident that might have been prevented by a technology option that was considered but not implemented.

Conclusions

Despite voluntary efforts by industry associations and a number of DHS programs to assist companies in protecting their chemical facilities, the extent of security preparedness at U.S. chemical facilities remains largely unknown. DHS does not currently have the authority to require the chemical industry to take actions to improve their security. On this basis, DHS has concluded—as we did in 2003 and again in January 2006—that its existing authorities do not allow it to effectively regulate chemical sector security. Since 2002, both DHS and EPA have called for legislation creating security requirements at chemical facilities, and legislation has been introduced without success in every Congress since September 11, 2001. By granting DHS the authority to require high-risk chemical facilities to take security actions, policy makers can better ensure the preparedness of the chemical sector. Furthermore, implementing inherently safer technologies potentially could lessen the consequences of a terrorist attack by reducing the chemical risks present at facilities, thereby making facilities less attractive targets. However, substituting safer technologies can be prohibitively expensive and can shift risks onto other facilities or the transportation sector. Also, in many cases, it may not be feasible to substitute safer chemicals or change to safer processes. Therefore, given the possible security and safety benefits as well as the potential costs to some companies of substituting safer technologies, a collaborative study employing DHS's security expertise and EPA's chemical expertise could

help policy makers determine the appropriate role of safer technologies in facility security efforts.

Contacts and Acknowledgments

For further information about this statement, please contact John B. Stephenson at (202) 512-3841. Karen Keegan, Omari Norman, Joanna Owusu, Vincent P. Price, and Leigh White made key contributions to this statement.

Appendix I: Overview of Key Chemical Security Legislative Proposals in the 109th Congress

Since 2001, the Congress has considered a number of legislative proposals that would give the federal government a greater role in ensuring the protection of the nation's chemical facilities. These legislative proposals would have granted DHS or EPA, or one of these agencies in consultation with the other, the authority to require chemical facilities to conduct vulnerability assessments and implement security measures to address their vulnerabilities. In the 109th Congress, five bills have been introduced but have not yet been acted upon: H.R. 1562, H.R. 2237, S. 2145, H.R. 4999, and S. 2486.

Major provisions	H.R. 1562	H.R. 2237	S. 2145 / H.R. 4999
General requirements	High-priority facilities would be required to submit vulnerability assessments and security plans to DHS; other chemical sources would be required to self-certify completion of assessments and plans and provide DHS copies upon request.	High-priority facilities would be required to submit vulnerability assessments and to certify that they have prepared prevention, preparedness, and response plans to EPA.	Designated chemical sources would be required to submit vulnerability assessments, security plans, and emergency response plans to DHS. The assessment and security plan would be required to address security performance standards established by DHS for each risk-based tier. Chemical sources would be required to self-certify completion of assessments and plans.
Role of DHS and EPA	DHS, in consultation with EPA, would identify high-priority categories of facilities; DHS would receive and review assessments and plans.	EPA, in consultation with DHS and state and local agencies, would identify high-priority categories of facilities; EPA would receive assessments and certifications.	DHS would designate facilities as chemical sources and assign each chemical source to a risk-based tier. DHS would receive and review assessments, plans and certifications. EPA would have no role.
Compliance enforcement	DHS would, when and where it deems appropriate, conduct or require the conduct of vulnerability assessments and other activities to ensure and evaluate compliance; DHS could disapprove a vulnerability assessment or site security plan; following written notification and consultation with the owner or operator, DHS could issue a compliance order.	Not later than 3 years after the deadline for submission of vulnerability assessments and response plans, EPA, in consultation with DHS, would review and certify compliance of each assessment and plan; following consultation with DHS, and 30 days after providing notification to the facility and providing advice and technical assistance to bring the assessment or plan into compliance and address threats, EPA could issue a compliance order.	DHS would review and approve or disapprove all vulnerability assessments, security plans, and emergency response plans for facilities in higher risk tiers within one year, and within five years for all other facilities. DHS would be required to disapprove of any vulnerability assessment, site security plan, or emergency response plan not in compliance with the vulnerability assessment, site security plan, and emergency response plan requirements. For higher risk facilities, if DHS disapproves the assessment or plans, the Secretary could issue an order to a chemical source to cease operation. For other facilities, the Secretary could issue an order to a chemical source to cease operation, but only after a process of written notification, consultation and time for compliance.

Major provisions	H.R. 1562	H.R. 2237	S. 2145 / H.R. 4999
Penalties for noncompliance	Would provide for court awarded civil penalties up to $50,000 per day for failure to comply with an order, site security plan, or other recognized procedures, protocols, or standards, and administrative penalties up to $250,000 for failure to comply with an order.	Would provide for court awarded civil penalties up to $25,000 per day, criminal penalties, and administrative penalties (if the total civil penalties do not exceed $125,000) for failure to comply with an order.	Would provide for court awarded civil penalties up to $50,000 per day, and administrative penalties of not more than $25,000 per day (not to exceed $1 million per year) for failure to comply with a DHS order or directive issued under the act. Also calls for criminal penalties of up to $50,000 in fines per day, imprisonment for not more than two years, or both for knowingly violating an order or failing to comply with a site security plan.
Inherently safer technologies requirements	None.	Response plans would be required to include a description of safer design and maintenance options considered and reasons those options were not implemented; EPA would be required to establish a clearinghouse for information on inherently safer technologies and would be authorized to provide grants to assist chemical facilities demonstrating financial hardship in implementing inherently safer technologies.	None.
Information protections	Would exempt information obtained from disclosure under the Freedom of Information Act (FOIA) or otherwise, or from disclosure under state or local laws; information would also not be subject to discovery or admitted into evidence in any federal or state civil judicial or administrative procedure other than in civil compliance action brought by DHS. Calls for DHS, in consultation with others, to establish confidentiality protocols.	Would exempt information obtained from disclosure under FOIA; calls for EPA, in consultation with DHS, to establish information protection protocols.	Would exempt information obtained from disclosure under FOIA, or from disclosure under state or local laws. Certifications submitted by the chemical sources, orders for failure to comply, and certificates of compliance and other orders would generally be made available to the public. Calls for DHS, in consultation with the Director of the Office of Management and Budget and appropriate federal law enforcement officials, to create confidentiality protocols for the maintenance and use of records; would establish penalties for the unlawful disclosure of protected information.
Equivalence of industry codes	Upon petition, DHS would be required to endorse other industry, state, or federal protocols or standards that the Secretary of DHS determines to be substantially equivalent.	None.	Would allow the Secretary to determine that vulnerability assessments, security plans, and emergency response plans prepared under alternative security programs meet the act's requirements and to permit submissions or modifications to the assessments or plans.

Major provisions	H.R. 1562	H.R. 2237	S. 2145 / H.R. 4999
Other	Would grant DHS right of entry; would exempt facilities that are subject to MTSA (port facilities) or the Bioterrorism Act (community water systems). Except with respect to protection of information, would not affect requirements imposed under state law.	Would grant EPA right of entry; would authorize EPA to provide grants for training of first responders and employees at chemical facilities; would not affect requirements imposed under state law.	Would grant DHS right of entry; would exempt facilities that are subject to MTSA from certain area security requirements but these facilities would otherwise comply with the act's requirements. Would preserve the right of States to adopt chemical security requirements that are more stringent than the Federal standard, as long as the State standard does not conflict with the Federal standard.

Source: GAO analysis of proposed legislation.

S. 2486, introduced on March 30, 2006, would impose a general duty on chemical facility owners and operators, in the same manner as the duty under the Clean Air Act's Section 112(r), to identify hazards that may result from a criminal release, ensure the design, operation, and maintenance of safe facilities by taking such actions as are necessary to prevent criminal releases, and eliminate or significantly reduce the consequences of any criminal release that does occur. S. 2486 also directs DHS to work with EPA, as well as state and local agencies, to identify not fewer than 3,000 high priority chemical facilities. These facilities would be required to take adequate actions (including the design, operation, and maintenance of safe facilities), to detect, prevent, or eliminate or significantly reduce the consequences of criminal releases and to submit a report to DHS that includes a vulnerability assessment; a hazards assessment; a prevention, preparedness, and response plan; statements as to how the response plan meets regulatory requirements and general duty requirements; and a discussion of the consideration of the elements of design, operation, and maintenance of safe facilities. "Design, operation, and maintenance of safe facilities" is defined as practices of preventing or reducing the possibility of a release through use of inherently safer technologies, among other things. DHS would certify compliance and DHS and EPA would establish a program to conduct inspections of facilities. The bill also provides for civil penalties, administrative penalties, and criminal penalties (including imprisonment for up to 2 years for first violations and up to 4 years for subsequent violations), for owners or operators of high priority facilities who fail to comply with an order.

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

- submit a report to the Senate and House Committees on Appropriations by February 10, 2006, describing (1) the resources needed to implement

mandatory security requirements for the chemical sector and to create a system for auditing and ensuring compliance with the security standards and (2) the security requirements and any reasons why the requirements should differ from those already in place for chemical facilities that operate in a port zone;

- complete vulnerability assessments of the highest risk U.S. chemical facilities by December 2006, giving preference to facilities that, if attacked, pose the greatest threat to human life and the economy; and

- complete a national security strategy for the chemical sector by February 10, 2006.[1]

[1]H.R. Conf. Rep. No. 109-24 (2005).

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

Congressional Relations

Gloria Jarmon, Managing Director, 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 (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548