



February 7, 2007

Dennis Deziel
Chief Program Analyst
Mail Stop 8610
Department of Homeland Security
Washington, DC 20528-8610

RE: Chemical Facility Anti-Terrorism Standards, Department of Homeland Security, DHS-2006-0073

Dear Mr. Deziel:

OMB Watch and Public Citizen appreciate the opportunity to comment on the Department of Homeland Security's (DHS) proposed Chemical Facility Anti-Terrorism Standards, published December 28, 2006. Section 550 of the Department of Homeland Security Appropriations Act of 2007 ("Section 550") requires DHS to develop security performance standards for high risk chemical facilities. Our comments outline several problems with the proposed regulations. In particular, we object to the regulation's excessive secrecy and impediments to information sharing, as well as the preemption of permanent state chemical security programs. Additionally, the omission of requirements to consider inherently safer technologies and a system to receive alerts and input from workers and communities are missed opportunities. We hope the Department considers our comments and makes the appropriate improvements in the finalized interim regulation.

OMB Watch is a nonprofit research and advocacy organization whose core mission is to promote government accountability and improve citizen participation. Public access to government information has been an important part of our work for more than 15 years, and we have both practical and policy experience with disseminating government information. For example, in 1989 we began operating RTK NET, an online service providing public access to environmental data collected by the Environmental Protection Agency. Additionally, we are engaged in agency regulatory processes and encourage agency rules to be sensible and more responsive to public needs.

Public Citizen is a national non-profit public interest organization with 100,000 members nationwide. We represent consumer interests through lobbying, litigation, regulatory oversight, research and public education.

The National Security Threat

Chemical facilities pose one of the greatest threats to our nation's security. There are 123 chemical plants that, if attacked, could endanger more than one million lives, more than 700 plants that place 100,000 people's lives at risk, and more than 3,000 facilities that place 10,000

people's lives at risk.¹ The U.S. Army's Surgeon General states that 2.4 million people are at risk of death or injury as a result of an attack on a chemical plant in the United States, and the U.S. Public Interest Research Group estimates that 41 million Americans live in "within range of a toxic cloud that could result from a chemical accident at a facility located in their home zip codes."²

Chemical plants storing deadly toxic chemicals are located near many of the most densely populated American cities, and the security at many of these facilities is notoriously lacking. The Agency for Toxic Substances and Disease Registry finds that security at chemical facilities range from "fair to very poor."³ The media has run numerous stories of reporters walking easily into chemical facility sites containing large tanks of dangerous toxic chemicals. For example, the Pittsburgh Tribune-Review's month-long probe into chemical plant security at 30 facilities in Baltimore, Chicago and Houston "found safeguards so lax that a potential terrorist can easily reach massive tanks of toxins that endanger millions of residents."⁴

The voluntary effort to increase security at chemical facilities has not worked. Given the severity of the threat, we expect a rigorous and thorough government program -- a program that seeks to increase security, improve safety and planning, and reduce the risk and consequences of major incidents at these facilities. In order to prevent an attack that could, according to a former member of the National Security Council, "approximate the world trade center," we need to ensure that the highest security is in place at the thousands of chemical facilities across the country.⁵

The Authorizing Legislation

Despite bipartisan progress on chemical security legislation in the 109th Congress, Section 550 was attached to an appropriations bill and passed. OMB Watch and Public Citizen have identified several shortcomings and limitations with the statutory language passed and outline the four most significant deficiencies below. While we realize that these aspects are outside of DHS's control, we believe it is important that the agency be aware of these problems in order to avoid compounding them with similar regulatory language in areas where the statute has left DHS greater flexibility.

Limited enforcement authority – Section 550(a) prevents DHS from "disapprov[ing] a site security plan submitted under this section based on the presence or absence of a particular security measure." In other words, DHS cannot mandate that a chemical facility implement a particular approach or measure to reduce their security risk. OMB Watch and Public Citizen disagree with this approach and believe that it restricts DHS—the organization in the best position to determine needed measures—from ensuring that facilities make the best progress possible. If a widely-practiced and cost-efficient procedure can severely reduce the risk posed

¹ James V. Grimaldi and Guy Gugliotta. "Chemical Plants Feared as Targets," *Washington Post*. December 16, 2001.

² Eric Pianin. "Study Assesses Risk of Attack on Chemical Plant," *Washington Post*. March 12, 2002; U.S. Public Interest Research Group. *Too Close to Home: Chemical Accident Risks in the United States*. 1998.

³ James V. Grimaldi and Guy Gugliotta. "Chemical Plants Feared as Targets."

⁴ Carl Prine, "Chemicals Pose Risks Nationwide," *Pittsburgh Tribune-Review*. May 5, 2002.

⁵ "In Sight: Chemical Targets," *National Journal*. August 10, 2003.

by a chemical facility, we believe that DHS should have the authority to deny a security plan if a facility has refused to include such a procedure.

Third party security programs – The statute allows for DHS to "approve alternative security programs established by private sector entities, Federal, State, or local authorities, or other applicable laws if the Secretary determines that the requirements of such programs meet the requirements of this section and the interim regulations." OMB Watch and Public Citizen believe that allowing the use of private sector chemical security certification forms and programs has the potential to create an uneven playing field and limits the potential of a robust chemical security program. The federal government should use its authority to create a mandatory robust chemical security program which is applied uniformly across the chemical sector. One of the greatest strengths of a federal program is the uniformity of requirements and information, which allow government personnel to identify important advances and missed opportunities. The submission of various forms and formats for the required information will make it more difficult for DHS to identify trends and patterns and could prohibit the agency from making fully-informed decisions on the sufficiency of company plans. Therefore, submission of information developed for such third-party programs should not be permitted under this program, except as additional information beyond the required federal reports. Trade associations and state programs should be encouraged to adapt to the federal government's requirements for private and regional chemical security program, but the federal government should not adapt to a private sector chemical security or state programs.

Excessive secrecy – OMB Watch and Public Citizen object to the broad secrecy provisions of Section 550(c). The bill states that, "vulnerability assessments, site security plans, and other information submitted to or obtained by the Secretary under this section, and related vulnerability or security information, shall be treated as if the information were classified material." We regard this provision as excessive, with little regard for the lessons learned from the 9/11 Commission about the importance of information sharing in a strong security program. The provision emphasizes concealing information as opposed to sharing information with other government agencies and with the public in a reasonable and responsible manner. Much of the information collected by DHS will include sensitive details that should be restricted from public access, but efforts should be made to provide access to some of the information, especially for communities living around dangerous facilities. Such communities have the right to be informed of the threats they face and the actions being taken by the government and by facilities to provide a greater level of security. Moreover, effective emergency response requires an informed citizenry that can actively assist in its own protection; the aftermaths of both the 9/11 attacks and Hurricane Katrina demonstrated this need. It is critical that citizens be informed of emergency procedures and safety instructions prior to the emergency, because communication during the chaos of a catastrophe is extremely limited. The legislation passed by Congress does little to increase the sharing of information between government agencies at the federal, state and local levels or with the public.

Limited scope – Section 550(a) instructs DHS to develop a chemical security program only for chemicals facilities that present a "high level of security risk." What high risk means is left for DHS to interpret, and we encourage DHS to make a generous interpretation of this provision. OMB Watch and Public Citizen believe that all facilities that store or process toxic chemicals are

a potential security and safety threat, and, as such, all of these facilities should be subject to a set of escalating standards. There should be a set of baseline security and safety standards that increase with the severity of the risk posed by facilities. We are also disappointed that Section 550(a) fails to cover facilities which are subject to the regulations of the Maritime Transportation Security Act of 2002, the Federal Water Pollution Control Act, or the Nuclear Regulatory Commission or any facilities which are operated by the Department of Defense or the Department of Energy. All facilities should be subject to the same baseline security requirements, and the first federal chemical security program should not make exceptions for facilities simply because they are operated by another agency or subject to another law. The security requirements will be different at these facilities, and we need to ensure that the chemical security requirements are, first, robust and, second, that they apply to all chemical facilities.

OMB Watch and Public Citizen hope that Congress will correct these limitations in any future chemical security legislation, and we urge DHS to consider these shortcomings, request that Congress fix them, and try to avoid compounding them with unsatisfactory regulatory language.

Proposed Interim Rule

Though the above provisions limit DHS's effectiveness, OMB Watch and Public Citizen believe that DHS has sufficient leverage to create a more robust chemical security program than was proposed. In what follows, we address the shortcomings of DHS's proposed interim regulations.

New SBU Category

One of the most troubling aspects about DHS's proposed rule is the establishment of impediments to information sharing. As noted above, OMB Watch strongly believes that limiting the free flow of information increases the danger faced by a terrorist attack upon a chemical facility. In the proposed rule DHS also acknowledges the problems associated with the proliferation of sensitive but unclassified (SBU) categories that restrict and slow information sharing. The rule states "the Department [of Homeland Security] recognizes that there are strong reasons to avoid the unnecessary proliferation of new categories of sensitive but unclassified information." Despite this acknowledgement, DHS proposes the creation of "a category of information for certain chemical security information called Chemical-terrorism Security and Vulnerability Information (CVI)." DHS states that information marked as CVI will be subject to restrictions similar to those of sensitive security information (SSI), which is "strictly limited to those persons with a need to know." The proposed regulation states that access to CVI is limited to "covered persons who have a need to know." OMB Watch and Public Citizen strongly object to this paradigm for information management, believing it to be a highly flawed paradigm for the post-9/11 world. The broad and vague wording will lend the new category to excessive use, and CVI restrictions will prevent timely sharing of needed information.

There are well-documented problems with SBU information categories. President Bush created the Information Sharing Environment (ISE) under the Director of National Intelligence to address these problems and develop a government-wide policy for SBU homeland security information. The ISE Implementation Plan states that, "the growing and non-standard inventory of SBU designations and markings is a serious impediment to information sharing among

agencies, between levels of government, and, as appropriate, with the private sector."⁶ Due to a lack of standardization, a lack of training, and a lack of explicitly stated policy, SBU information categories create confusion among agencies, unnecessary controls and an inability to promptly share critical information.

The General Accountability Office noted that the now over 100 SBU information categories have created problems for those at the local levels. First responders, for instance, "reported that the multiplicity of designations and definitions not only causes confusion but leads to an alternating feast or famine of information."⁷ First responders and others may need to quickly access information collected under this program, but by creating a new and poorly defined category of restricted information, DHS has made it likely that bureaucratic procedures could easily slow or even prevent sharing of information with key users. Instead of creating a new broad category of controlled information that could easily expand to include a wide variety of unintended health and safety information and slow sharing of important information, OMB Watch and Public Citizen recommend DHS identify a limited list of specific information that will be restricted from public access. No other information would be guaranteed restriction from public access under this chemical security program, and should instead be placed in an information sharing system.

However, if DHS retains the CVI approach to information management, then OMB Watch and Public Citizen recommend the following clarifications to CVI in order to limit the problems typically associated with SBU categories:

- The regulation should clearly state the required standards for marking a document or portion of a document as CVI. Without clearly stated policy, the risk of inappropriate markings is increased, and unnecessary information controls are put into place.
- A clear distinction should be drawn between Freedom of Information Act (FOIA) exemptions and CVI to demonstrate that a CVI marking is not a sufficient justification for FOIA exemption and that a FOIA request for a document marked as CVI should proceed according to normal FOIA review procedures.
- A process should be established to challenge and appeal CVI markings. Since many SBU categories have grown to inappropriately include information that should legitimately be available to the public, the management of CVI should include procedures that allow those denied information to challenge the information's inclusion in the CVI category.
- There should be an expiration date on information marked as CVI, just as there is an expiration date on classified information. OMB Watch and Public Citizen recommend the use of a 5-year expiration date that can be renewed by the Secretary of DHS.
- The regulation should limit who may hold the authority to mark a document as CVI. At many agencies using SBU information categories, the lack of such limitations has led to government employees, contractors and even companies submitting the information

⁶ Program Manager, Information Sharing Environment. *Information Sharing Environment Implementation Plan*. November 2006, p. 94.

⁷ General Accountability Office. *Information Sharing*. GAO-06-385, March 2006, p. 25.

unnecessarily marking and forcing the agency to control voluminous amounts of information.⁸

- DHS should establish a training program to fully brief implementing personnel on the procedures and limitations of the CVI program.
- DHS should include commitments to regularly report to Congress on the number of documents marked as CVI, the cost of implementing CVI policies and of safeguarding documents so marked, and the number, training, and levels of officials with authority to designate information as CVI. Additionally, the DHS Inspector General should annually audit the chemical security program and CVI information management for the three years the temporary regulations are in place.
- If the CVI policy is not fully developed in this regulation, then DHS should commit to providing an opportunity for public to participate in the policy development and implementation planning. The public has a vital interest in CVI, and the public should have an opportunity to comment on proposed CVI policy.
- The regulation should include provisions which protect whistleblowers. CVI policy should state that no criminal charges are associated with disclosing information marked as CVI in manner complying with whistleblower protections. CVI policy should also make clear that a CVI marking in no way bars disclosure to Congress or to an authorized official of an executive agency of information that is essential to reporting a violation of law, waste, fraud, abuse or other misconduct.

Information Sharing System

In order to prevent a potentially catastrophic event or to recover from such an event, DHS needs to develop robust information systems for two-way communication and maximize the amount of information that can be shared in these channels. In testimony before the Committee on Homeland Security, Lee Hamilton, former Vice Chair of the 9/11 Commission, plainly stated: "Poor information sharing was the single greatest failure of our government in the lead-up to the 9/11 attacks."⁹ To remedy the problem, Hamilton concluded that the government had to change its approach to information collection and control:

The 9/11 story included numerous examples of how a mentality of limiting information sharing to those with a 'need to know' in fact kept information from getting to the right people at the right time. Cultures will not change without policies in place that actively encourage such change, and without the sustained implementation of those policies.¹⁰

Unfortunately, DHS's proposed rule on CVI is a policy which will not encourage such change. In fact, by limiting information to those who "need to know," it promotes the pre-9/11 framework. Such a framework assumes that DHS officials can accurately and quickly determine who needs to know CVI information and what CVI information they need. The reality is that it is almost impossible to meet such expectations, and the most likely outcome is that agencies and individuals that need CVI information will be unable to get it. Instead, there needs to be a sustained effort to more widely share information regarding vulnerabilities at chemical facilities

⁸ See Ibid.

⁹ Prepared Statement of Lee H. Hamilton before the Committee on Homeland Security, U.S. House of Representatives, November 8, 2005, p. 1.

¹⁰ Ibid., p. 5.

among federal, state and local governments and with the private sector and the public. Such effort is not evident in the proposed rule, and we encourage DHS to create the infrastructure to increase information sharing, not by limiting information to those who "need to know," but by creating an environment and culture at DHS which understands the need to share information with state, local and private actors and with the public.

Scope of Information Restricted

OMB Watch and Public Citizen believe that DHS's chemical security program needs to provide greater public oversight and accountability. According to the proposed regulations, the following items will remain secret from the public:

- Chemical facility site security plans
- Standards for determining the risk level of chemical facilities
- Risk level of particular chemical facilities
- Vulnerabilities of chemical security plants
- Acceptance or denial of chemical facility site security plans
- Documents and notes relating to the auditing of chemical facilities

Currently the proposed regulation states that CVI covers vulnerability assessments, which include threat assessment, vulnerability analysis, risk assessment and countermeasures analysis.¹¹ In gathering materials to perform these analyses, DHS will rely upon programs run by the Environmental Protection Agency and the Occupational Safety and Health Administration, among others, and the documents, reports and materials they produce. DHS, according to the proposed rule, would have the authority to mark any information used in vulnerability assessment as CVI, including information produced by EPA and OSHA. The regulation should clearly state that information developed under other requirements of law or regulation cannot be restricted as CVI under this program.

People who live near chemical facilities have a right to know if they are living in safety and if their family's lives are in danger. We recognize that the site security plan should not be disclosed to the public nor should specific vulnerabilities be publicized, but a certain level of public access should be provided. After all, the program is designed to ensure the public's protection. Accordingly, OMB Watch and Public Citizen recommend that DHS provide the following information to the public.

The number and identity of chemical facilities covered by the program, the number and identity of facilities that have been certified by DHS and the number and identity of facilities that have had their site security plans denied by or are waiting for approval from DHS should be made available to the public. While some remain concerned that such information will be misused by terrorist for targeting of facilities, the reality is that the location and identity of dangerous facilities is publicly available information that cannot be made secret. This basic information should be publicly released to create an accountable chemical security program. Since this information cannot be hidden and is fundamental to informing the public about progress in this area, the government should not waste time and resources trying to restrict it.

¹¹ §27.400 and §27.225 of the Proposed Chemical Facility Anti-Terrorism Standards.

While OMB Watch and Public Citizen recommend that the approval and denial of site security plans should be made public, we wish to clarify that the reasons for denials should not be made public for reasons of national security. Those living around a facility have a right to know if the security plan of a facility down the street has been approved by DHS. Properly organized, the process can even create a strong incentive for companies to quickly remedy any problems identified by DHS. For instance, DHS could establish a one-month grace period during which the denial of a plan would not be made public. If, during this period, the company improved the deficiency cited by DHS in the denial, then the agency could rescind the denial prior to its being made public. This option to avoid a public reprimand would be a strong motivator for laggard facilities to improve. Publicizing the acceptance or denial would allow for public oversight and accountability and create pressure on facilities to get their plans approved.

DHS should also commit to publicly sharing trends and examples of best practices for site security and safety. DHS's role of central reviewer of the site security plans and vulnerability assessments places the agency in the unique position to track and evaluate such activities. Such information would be most useful on a broad sector-by-sector basis, without any information identifying specific facilities. This type of information would help inform facilities of new and better ways to improve operations and would empower those conducting oversight, such as state or local officials.

Overreaching and Counter Productive Preemption of State Law

The proposed chemical security interim regulation states that no state law or regulation can have any effect if it conflicts with the Department's regulations:

No law or regulation of a State or political subdivision thereof, nor any decision rendered by a court under state law, shall have any effect if such law, regulation, or decision conflicts with, hinders, poses an obstacle to or frustrates the purposes of these regulations or of any approval, disapproval or order issued thereunder.

DHS goes on to state that Section 550, "compels the Department to preserve chemical facilities' flexibility to choose security measures to reach appropriate security outcomes." By requiring DHS to implement a risk-based standard, requiring layered security plans and preventing DHS from rejecting a site security plan on the basis of the presence or absence of particular security measures, Congress struck a careful balance in regulating chemical security risk.

DHS suggests that if a state regulation is stronger than the DHS regulation, then it could potentially frustrate DHS's regulations, and the state regulation therefore can have no "effect." OMB Watch and Public Citizen strongly disagree with DHS's expansive interpretation of its authority under Section 550 and with its attempt to preempt the right of states to provide additional protections for their own citizen, which may include particularly vulnerable populations or, through the state courts, to deem dangerous companies negligent.

Certain states face unique threats due to the proliferation of chemical facilities in densely populated regions. In New Jersey, there are six industrial facilities that could endanger the lives

of one million people and fifteen that could endanger 100,000 or more people.¹² The FBI has called a two-mile stretch of New Jersey the "most dangerous two miles in America."¹³ As a result, New Jersey has stronger chemical security measures that require facilities that use the most toxic chemicals to investigate whether they could reduce or replace those chemicals. OMB Watch and Public Citizen believe that states have a right to pursue such efforts to protect their citizens against threats of chemical accidents or attacks and that DHS should not attempt to preempt this right.

OMB Watch and Public Citizen object to instituting a temporary program that blocks permanent state programs. Section 550(b) clearly instructs DHS to issue *interim* regulations that, "shall terminate three years after the date of enactment of this Act." It is clear from the statutory language, coupled with the legislative history of strong bipartisan progress on comprehensive chemical security bills, that Congress passed Section 550 only as a temporary fix. This program is meant to fill this gap until Congress can pass more comprehensive chemical security legislation. It makes no sense for DHS to shut down permanent state chemical security programs under a temporary program.

DHS's chemical security regulations should be viewed as a floor, not a ceiling. Vulnerabilities at chemical facilities across the country differ due to different sizes of populations around dangerous chemical facilities and different quantities and levels of toxicity of chemicals at facilities. DHS has issued a modest proposal for ensuring the security of certain high-risk chemical facilities. This should not and cannot prevent responsible states from ensuring the protection of their citizens in high risk areas. Regulations which provide greater security to cover particularly vulnerable regions should remain in effect.

Lack of Authority to Preempt State Law

OMB Watch and Public Citizen also point out that DHS lacks the authority to preempt state law. The power to preempt state law derives from Article VI, Section 2 of the U.S. Constitution which states that the Constitution and federal laws are the "supreme Law of the Land." Courts have traditionally sided with states in cases involving disagreements about preemption. According to case law, the power to preempt state law can take one of two forms: express preemption or implied preemption.

Express preemption is when Congress explicitly states that legislation preempts conflicting state law. It is clear that Section 550 does not expressly preempt state law. Moreover, Congress considered including a preemption provision and rejected it. Sen. George Voinovich (R-OH) introduced a preemption provision as an amendment but later withdrew it due to Congressional opposition. The original House and Senate chemical security bills did not include a preemption provision. Though neither of these bills ever became law, it is clear that Congress never decided to preempt state law when it did enact federal chemical security legislation.

¹² New Jersey Work Environment Council. "Press Release: WEC report: New Jersey chemical catastrophe could harm millions," May 23, 2006.

¹³ "David Kocieniewski. "Corzine's Chemical Security Stance Draws Scrutiny a Year Into His New Job," *The New York Times*. December 28, 2006.

According to case law, implied preemption applies in one of three situations. First, conflict preemption occurs when it is impossible to comply with both federal and state law. DHS can not claim a conflict preemption theory applies in this instance, because it is possible for chemical facilities to comply with both federal and with state chemical security regulations and law. Even if state regulations are stronger, this does not create a conflict, because it is possible for facilities to operate in compliance with federal laws and regulation. Second, preemption can occur when federal law occupies the field; that is, when it is the intent of Congress is for federal legislation to be exclusive. The legislative history makes clear that in this case, Congress did not intend for Section 550 to be exclusive. As noted above, Congress was aware of state regulations and chose not to enact preemptive language. Third, implied preemption can occur when the objective of federal legislation is impeded by state legislation. This is what DHS argues.

DHS claims that the objective of Congress was to create a chemical security program which “preserve[s] chemical facilities' flexibility to choose security measures to reach appropriate security outcomes.” If a state law prevents a chemical facility from exercising such flexibility, then, according to DHS, the state law will have impeded the objective of Congress.

This argument is flawed and relies on legerdemain. No provision of Section 550 states that chemical facilities should have the flexibility to choose security measures. The wording of the provision is, "That such *regulations* shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility" (emphasis added).

The provision merely requires that DHS's own regulations impose somewhat flexible security measures; it does not address the interaction of state requirements and the federal scheme. Congress's objective of a flexible federal regulatory program is in no way impeded by strong state chemical security regulations, because the content of a state rule need not change what DHS identifies as the components for its site security plan rules. Therefore, DHS lacks implied preemption authority.

Moreover, citizens also clearly have a right to address chemical company negligence through a state's court system and retain a constitutional right to a jury trial under the 7th Amendment to the U.S. Constitution and numerous state constitutions. Congress did not delegate to the DHS any power to make the *ultra-vires* determination that preemption of state common law claims is either authorized or warranted.

OMB Watch and Public Citizen strongly advise that DHS remove the preemption provisions from its finalized interim regulations.

Consideration of Inherently Safer Technology

OMB Watch and Public Citizen urge DHS to add provisions to the regulation which strongly encourage chemical facilities to consider implementing safer processes and using safer chemicals as a method to improve site security through the reduction of risk. Such provisions would not force companies to implement inherently safer technologies nor would they establish a litmus test to reject site security plans simply based on the absence of inherently safer technologies

from the plan. The provisions would merely add a section to companies' site security plans which analyze alternatives for lowering the risk of a chemical attack through the implementation of safer procedures, technologies or chemicals. Companies should be encouraged to consider other options which will greatly reduce their security risks.

Third Party Certification Process

As noted above, DHS is given the authority to approve site security plans which are submitted through third parties (*e.g.*, private sector industry associations). OMB Watch and Public Citizen believe that exercising such an allowance will create an uneven playing field. Large segments of chemical security facilities that submit plans in different formats could result in a system which makes it difficult for DHS to consistently and informatively review and evaluate site security plans. While the statutory language allows for DHS to accept such third party programs, it does not require that the agency do so and leaves the final decision to DHS. If businesses are concerned about duplication and overburdening companies with multiple forms, then industry associations should be required to adopt programs which comply with federal forms and regulations. OMB Watch and Public Citizen, therefore, encourage DHS not to accept any private sector certification programs in substitution for the federal chemical security program. All companies should be held to precisely the same standards and requirements.

Community and Worker Participation

The proposed regulations fail to include a role for workers at chemical facilities or communities located around chemical facilities. Such individuals have access to a great deal of information regarding the operations and safety of chemical facilities. Police, fire fighters and other emergency personnel may often notice problems or issues that facilities overlook, deemphasize or even intentionally avoid in their site security plans. DHS should, therefore, create procedures for involvement of workers and community representatives during the development and approval of chemical site security plans. Additionally, DHS should create a system that allows individuals to report vulnerabilities, shortcomings, and failures to implement security plans directly to DHS officials without fear of reprisals or retaliation from the company.

Summary: Recommendations

OMB Watch and Public Citizen recommend that DHS make the following revisions to the interim chemical facility anti-terrorism regulations:

- Replace the Chemical-terrorism Security and Vulnerability (CVI) policy with a limited list of specific information that will be restricted from public disclosure.
- If the CVI is retained,
 - The regulation should include clear standards for marking a document or portion of a documents as CVI.
 - A savings provision should be added to the regulation stating that CVI will not impede the operations of existing state or federal programs.
 - There should be a training program for appropriately marking documents as CVI.
 - The regulation should include a review process and a public appeals process.

- Provisions should clarify that CVI markings do not automatically make information exempt from FOIA and that CVI materials should be reviewed according to normal FOIA review procedures.
 - There should be an expiration date on information marked as CVI, just as there is an expiration date on classified information.
 - Clear limits should be placed on who is authorized to mark a document as CVI.
 - There should be a public role in CVI policy development and implementation process.
 - DHS should regularly report on the CVI program and have the inspector general annually audit the program.
 - The regulation should include a clear statement to whistleblower protections apply to those disclosing CVI information consistent with protected whistleblower procedures and that CVI markings in no way bars disclosure to Congress.
- Make a commitment to publicly disclose the number and identity of chemical facilities covered by the program, as well as the number and identity of facilities that have been certified by DHS and those that have had their site security plans denied.
 - Publicly disclose the approval and denial of site security plans but not the reasons for denials for reasons of national security.
 - Commit to publicly report the best practices of site security plans on a sector-by-sector basis.
 - Remove section 27.405 of the proposed regulation, which attempts to preempt state chemical security regulations and common law rights.
 - Add provisions to encourage chemical facilities to consider implementing safer processes and using safer chemicals.
 - Not accept any private sector certification programs in substitution for the federal chemical security program.
 - Create procedures to involve workers and community members in the development and approval of the site security plan.
 - Develop a system to allow individuals to report vulnerabilities, shortcomings and failures in implementation to DHS.

We hope DHS implements these recommendations in the finalized interim chemical security regulations.

Sincerely,



Sean Moulton, Director of Federal
Information Policy
OMB Watch



Clayton Northouse, Information Policy
Analyst
OMB Watch



Laura MacCleery
Director, Congress Watch
Public Citizen