THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 11

MAY 2007

CHEMICAL SECTOR

Click **here** to subscribe. Visit us online for this and other issues at http://cipp.gmu.edu

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This month's issue of *The CIP Report* is focused on the chemical sector, which has recently seen a flurry of activity regarding new regulations. The Chemical Sector is one of the oldest and most mature critical infrastructure sectors and is broadly defined to include chemical manufacturing, transportation, and storage/use of chemicals and all those involved in these processes. Prior to the release of the Interim Rule Standards imposing comprehensive federal security regulations for high risk chemical facilities on April 2, 2007, the majority of regulations within this sector directly impacting security were targeted towards environmental protection and the transportation of hazardous materials. In a sector long concerned with safety and accident prevention, other security initiatives have been primarily sector-led, relying on organizations such as the American Chemistry Council.

The chemical sector's Sector Specific Agency is the Department of Homeland Security, Office of Infrastructure Protection. The Chemical Sector Information Sharing and Analysis Center was formed in 2002 and enables the sector to receive access to sensitive information about cyber, physical and contamination issues deemed to have possible serious national security, economic, or social consequences. The Chemical Sector ISAC uses CHEMTREC, the chemical industry's 24-hour emergency communication center, as the communication link between the Department and ISAC participants. The sector has long since recognized the importance of cyber security to overall security, and in 2002 formed the Chemical Sector Cyber Security Program, which draws upon well established programs to provide a coordinated approach to enhancing cyber security practices.

In this issue, we highlight a number of programs and organizations that have responded to these regulations or are involved in actively organizing the Chemical sector's security practices. In addition to some background information on the new Anti-Terrorism Standards, we have included excerpts from the briefing given by Secretary Chertoff, as well as portions of the Interim Rule Standards on risk assessment, and brief overviews of the Chemical Sector Coordinating Council, the Cyber Security Industry Alliance's Report on Chemical Plant Security, the Chemical Sector Cyber Security Program, and the impact of the federal regulations on states. In addition to these pieces, we have also included responses to the Interim Rule Standards from the American Chemistry Council, the American Council on Education, and a Legal Insights column that further examines the impact of these new regulations.

As always, we appreciate your continued support of the CIP Program.

John A. McCarthy
Director, CIP Program
George Mason University, School of Law

U.S. Chemical Facilities Face New Anti-Terrorism Standards

The U.S. Department of Homeland Security has released an interim final rule that imposes comprehensive federal security regulations for high risk chemical facilities. This rule establishes risk-based performance standards for the security of our Nation's chemical facilities.

Summary

The Department of Homeland Security (DHS or Department) issues this interim final rule (IFR) pursuant to Section 550 of the Homeland Security Appropriations Act of 2007 (Section 550), which provided the Department with authority to promulgate "interim final regulations" for the security of certain chemical facilities in the United States.

This rule establishes risk-based performance standards for the security of our nation's chemical facilities. It requires covered chemical facilities to prepare Security Vulnerability Assessments (SVAs), which identify facility security vulnerabilities, and to develop and implement Site Security Plans (SSPs), which include measures that satisfy the identified risk-based performance standards. It also allows certain covered chemical facilities, in specified circumstances, to submit Alternate Security Programs (ASPs) in lieu of an SVA, SSP, or both.

The rule contains associated provisions addressing inspections and audits, recordkeeping, and the protection of information that constitutes Chemical-terrorism Vulnerability Information (CVI). Finally, the rule provides the Department with authority to seek compliance through the issuance of Orders, including Orders Assessing Civil Penalty and Orders for the Cessation of Operations.

Statutory Regulatory Authority and History

Under the new regulations, high-risk chemical facilities will be required to identify vulnerabilities and develop Site Security Plans.

On October 4, 2006, the President signed the Department of Homeland Security Appropriations Act of 2007 (the Act), which provides the Department of Homeland Security with the authority to regulate the security of high-risk chemical facilities. (*See Pub. L. 109-295, sec. 550.*) Section 550 requires the Secretary of Homeland Security to promulgate interim final regulations "establishing risk-based performance standards for security of chemical facilities" by April 4, 2007. Although interim final regulations are usually issued without prior notice and comment (and the Act requires neither), the Department issued an Advance Notice of Rulemaking (Advance Notice) seeking comment on the significant issues and regulatory text.

Appendix A: DHS Chemicals of Interest

In this interim final rule, the Department has decided to evaluate chemical facility risks by, in part, classifying facilities by particular chemicals. In proposed Appendix A, the Department has included a list of "DHS Chemicals of Interest" along with Screening Threshold Quantities, or STQs, for each chemical.

In addition to drawing on information from existing sources, the Department has identified chemicals by considering three security issues. These three security issues, which are explained below, address multiple risk areas.

1. **Release:** DHS believes that certain quantities of toxic, flammable, or explosive chemicals or materials, if released from a facility, have the potential for

(Continued on Page 3)

"Now, it's obviously very important to the economy that we have a chemical sector that is capable of functioning and being prosperous, but it's also true that we know that the aggregation or the collection of a lot of potentially dangerous chemicals in one place does create an attractive target to somebody who wants to carry out a terrorist attack." Secretary of Homeland Security Michael Chertoff

Facilities *(Continued from Page 2)*
significant adverse consequences for human life or health.

2. **Theft or Diversion:** DHS believes that certain chemicals or materials, if stolen or diverted, have the potential to be used as weapons or easily converted into weapons using simple chemistry, equipment or techniques in order to create significant adverse consequences for human life or health.

3. **Sabotage or Contamination:** DHS believes that certain chemicals or materials, if mixed with readily-available materials, have the potential to create significant adverse consequences for human life or health.

In proposed Appendix A, the Department lists the DHS Chemicals of Interest and identifies a Standard Threshold Quantity (STQ) for each chemical. To clearly identify each chemical, the Department includes the Chemical Abstract Service (CAS) number for each chemical. These chemicals listed in proposed Appendix A fall into the three categories identified above: chemicals with a release hazard, chemicals with a theft or diversion hazard, and chemicals with a sabotage or contamination hazard.

The Department acknowledges that there are two additional security issues that it is considering at this time, although it is not including any such chemicals that would trigger a Top-Screen submission. They include the following two issues:

1. **Critical Relationship to Government Mission:** DHS believes that the loss of certain chemicals, materials, or facilities could create significant adverse consequences for national security or the ability of the government to deliver essential services.

2. **Critical Relationship to National Economy:** DHS believes that the loss of certain chemicals, materials or facilities could create significant adverse consequences for the national or regional economy.

The Advance Notice defined "Chemical Facility or facility" to mean "any facility that possesses or plans to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criterion identified by the Department.

The Department is continuing to assess currently-available information about these chemicals critical to government mission and the national economy. The Department will use the information it collects through the Top-Screen process, as well as currently-available information, as a means of identifying facilities responsible for economically critical and mission-critical chemicals. ❖

Interim Rule Standards on Risk Assessment

Security Vulnerability Assessments (Sec. 27.215)

Initial Assessment. If the Assistant Secretary determines that a chemical facility is high-risk, the facility must complete a Security Vulnerability Assessment. A Security Vulnerability Assessment shall include:

(1) Asset Characterization, which includes the identification and characterization of potential critical assets; identification of hazards and consequences of concern for the facility, its surroundings, its identified critical asset(s), and its supporting infrastructure; and identification of existing layers of protection;
(2) Threat Assessment, which includes a description of possible internal threats, external threats, and internally-assisted threats;
(3) Security Vulnerability Analysis, which includes the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and in meeting the applicable Risk-Based Performance Standards;
(4) Risk Assessment, including a determination of the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a success of an attack; and
(5) Countermeasures Analysis, including strategies that reduce the probability of a successful attack or reduce the probable degree of success, strategies that enhance the degree of risk reduction, the reliability and maintainability of the options, the capabilities and effectiveness of mitigation options, and the feasibility of the options.

Site Security Plans (Sec. 27.225)

The Site Security Plan must meet the following standards:

(1) Address each vulnerability identified in the facility's Security Vulnerability Assessment, and identify and describe the security measures to address each such vulnerability;
(2) Identify and describe how security measures selected by the facility will address the applicable risk-based performance standards and potential modes of terrorist attack including, as applicable, vehicle-borne explosive devices, water-borne explosive devices, ground assault, or other modes or potential modes identified by the Department;
(3) Identify and describe how security measures selected and utilized by the facility will meet or exceed each applicable performance standard for the appropriate risk-based tier for the facility; and
(4) Specify other information the Assistant Secretary deems necessary regarding chemical facility security.

Risk-based Performance Standards (Sec. 27.230)

Covered facilities must satisfy the performance standards identified in this section. The Assistant Secretary will issue guidance on the application of these standards to risk-based tiers of covered facilities, and the acceptable layering of measures used to meet these standards will vary by risk-based tier. Each covered facility must select, develop in their Site Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:

(1) Restrict Area Perimeter. Secure and monitor the perimeter of the facility;
(2) Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;
(3) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter.
(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;
(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;
(7) Sabotage. Deter insider sabotage; *(Continued, Page 14)*

Statement by American Chemistry Council Urging Congress to Allow DHS to Implement Security Regulations

After several years of debate, the federal government is finally ready to implement national chemical security regulations that will build on the accomplishments of industry and state programs to protect the nation's chemical facilities and communities from a terrorist attack. Congress should support these new regulations and reject language inserted into the now vetoed Iraq spending bill that would allow states to enforce rules that are stricter than federal rules regarding security at chemical facilities. Proponents of the language fear that the new federal rules could pre-empt states from implementing stricter security laws in the future. But opponents say that such language only weakens the federal government's ability to effectively regulate chemical security.

American Chemistry Council President & CEO Jack N. Gerard issued the following statement:

Prior to government action, ACC members set the bar by voluntarily spending more than $3.5 billion to enhance security at nearly 2,000 facilities since 2001. Our industry program has served as a model for existing state programs like New Jersey and we continue to fully support federal regulations.

We consistently make the point with members of Congress that these unnecessary and unwise provisions inserted in the Iraq spending bill will weaken the federal government's ability to work with state governments and industry to protect the nation's chemical facilities and communities from a terrorist attack.

The provisions are based on a false premise that there is need for Congress to act in order to preserve existing state chemical security programs. Since the regulations were issued in April by the Department of Homeland Security, it has become quite clear they will not invalidate existing chemical security state programs or prevent a state from improving their program. Even the State of New Jersey recognizes the new rules could preempt state or local requirements only if there is an actual conflict or the program "frustrates the purpose" of the federal program.

The Department of Homeland Security has struck a necessary and reasonable balance on possible preemption of state and local laws by following the precedent set by existing national security laws for aviation, nuclear, rail and port security. In fact, Congress continues to support this level of federal preemption on national security issues through recently introduced legislation addressing rail security. There is no compelling reason to treat the security of critical chemical facilities differently.

As President and CEO of ACC, Mr. Jack Gerard is leading new efforts to redefine the chemistry industry and strengthen its role in advocating public policy. He has pledged to make the ACC the "gold standard" of trade associations.

Federal preemption provides clarity to ensure facilities fully understand their regulatory obligations under both state and federal programs. More importantly, it ensures that federal and state programs operate in harmony to achieve the shared goal of enhancing security.

When Congress revisits this legislation following an expected veto by the President, we urge Congress to remove these unnecessary provisions that will only interfere with the Department of Homeland Security's ability to successfully secure the nation's high-risk chemical facilities." ❖

The American Chemistry Council (ACC) was created in 1872 and currently counts over 120 member companies. The mission of the ACC is "to deliver business value to its members through exceptional advocacy based on enhanced member performance, high quality scientific research, communications, effective participation in the political process, and a commitment to sustainable development through member contributions to economic, environmental and societal progress."

Legal Insights

Information Sharing and the New Chemical Security Regulations

Tim Clancy
Principal Research Associate for Law , CIP Program

Last year Congress mandated new regulations to secure high-risk chemical facilities in Section 550 of the Homeland Security Appropriations Act, 2007 (P.L. 109-295) (the Act) and DHS issued an interim final rule (IFR) in April. Controversy in Congress and State legislatures over whether these new regulations preempt State chemical security laws has overshadowed another issue: whether the new rules help or hinder information sharing between federal, state and local governments.

The federal government relies on state and local first-responders to help protect against acts of terrorism, but first responders often need access to sensitive security information possessed by the federal government to fulfill their homeland security mission. However, in the case of the new chemical security rule greater emphasis is placed on protecting information gathered by DHS and less on improving mechanisms for information sharing. Information sharing with State and local officials is not prohibited, but it is severely constrained under the new DHS regulations.

In Section 550 Congress spelled out several steps to restrict chemical facility security information from disclosure to the public. Any information generated under the Section shall be given protections from public disclosure consistent with similar information developed by chemical facilities regulated under Maritime Transportation Security Act of 2002 (MTSA). MTSA classifies chemical facility security information as sensitive security information, not to be publicly disclosed. Also, in any proceeding to enforce the law, any information submitted to or obtained by DHS under Section 550 shall be treated as if the information were classified material.

The Act does not require that DHS share chemical security information with state and local governments. Rather Section 550(c) says that such information sharing is not prohibited, while giving the DHS Secretary discretion to share chemical security information only with State and local government officials possessing necessary security clearances.

In response to Section 550, DHS issued regulations creating a new category of protected information called Chemical-terrorism Vulnerability Information (CVI). CVI is a complex regime that broadly defines what chemical security information is protected and narrowly restricts access to CVI to persons defined by DHS as those with a "need to know". According to the regula-

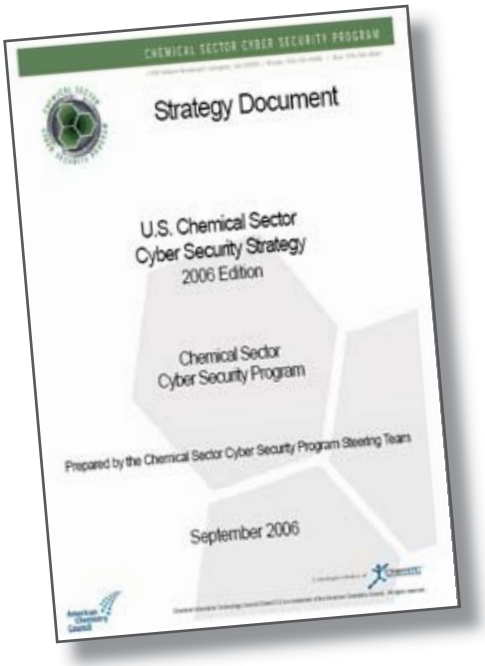
(Continued on Page 14)

Timothy P. Clancy is the new Principal Research Associate for Law, and the head of the Law Team at the CIP Program. He received his J.D. from Western New England College School of Law in Springfield, MA where he was a member of the Law Review. Tim also holds a B.A. in Political Science from the College of the Holy Cross in Worcester, MA.

Tim was formerly Chief of Staff to Representative Sherwood Boehlert (R-NY) while serving concurrently as Project Director for the Committee on Science of the U.S. House of Representatives. On the Science Committee, he helped coordinate Committee efforts in information security and homeland security R&D, resulting in the drafting of H.R. 3394 (P.L. 107-305), the Cybersecurity Research and Development Act of 2002 and Titles II and III of H.R. 5005 (P.L. 107-296), the Homeland Security Act of 2002. Tim also spent over six years at the National Science Foundation as Senior Legislative Policy Analyst in the NSF Office of Legislative and Public Affairs. Tim's primary research interests are in science and technology policy, higher education policy and the intersection of science, technology, security and the law.

Chemical Sector Cyber Security Program

Building upon a long focus on safety and security within the Chemical Sector, the Chemical Sector Cyber Security Program was organized in recognition of the increasing reliance of the sector on integrated IT manufacturing control systems, the continued threat of viruses, increasing usage of the Internet, and the growth of e-business. In the early 2000's, CIO's throughout the sector realized the need for a sector-wide strategy to address the cyber security issues and released the first Chemical Sector Cyber Security Strategy in 2002, which was appended to the National Strategy to Secure Cyberspace in February 2003.



Since that time, the sector has examined its progress against the 2002 Strategy and in September of 2006, released an updated document that continues to focus on cyber security risk management and reduction, leveraging collective knowledge and shared technology to improve the overall cyber security practices of the sector. The 2006 strategy is divided into five key elements.

Information Sharing

The Program encourages continued participation with information sharing groups, such as the US Computer Emergency Readiness Team (US-CERT), Homeland Security Information Network (HSIN), Business Roundtable CEO Com Link, and the Government Emergency Telecommunications Service (GETS). Additionally, the Program provides opportunities for professionals to share experiences and address common issues, as well as define processes for sharing information during a high impact incident.

Guidance Enhancement and Relevance

The Program evaluates cyber security preparedness leveraging the Chemical Industry Data Exchange (CIDX®), in addition to periodically reviewing and assessing existing guidance documents to evaluate their relevancy to current conditions and future needs.

Sector-wide Adoption

Working through the Chemical Sector Coordinating Council, the Program focuses on wide-spread adoption and implementation of the cyber guidance and tools, as well as forging relationships with international chemical companies, and creating a sector performance tool to evaluate, measure and report cyber security progress.

Enhanced Security in Technology Solutions

Working with IT product and service providers to better understand the sector's technology and security needs, the Program will explore key technology needs and form relationships with other sectors to help influence government research priorities and promote technology needs and issues.

Government Relations

The Program has invested in building strong relationships with DHS to ensure that the sector's cyber security initiatives are aligned with DHS priorities. In addition to the relationship with DHS, the sector focuses on building new relationships with local, state and other federal agencies to better connect the Chemical Sector's innovation with government expertise to reach the ultimate goal of a safe and secure cyberspace.

More information on the Chemical Sector Cyber Security Program and the 2006 Strategy is available at http://www.chemicalcybersecurity.com/program/. ❖

Concerns Remain about the Preemption of State Chemical Security Standards

Elizabeth Jackson, CIP Program

The topic of federal chemical security regulations is not new to Congress nor the Federal agencies charged with leading the protection of the Chemical Sector. For years, efforts were made to institute federal regulations, but only voluntary measures were adopted. These efforts were often derailed due to industry opposition, and faced intense scrutiny over the use of provisions regarding preemption and inherently safer technology (IST).

Not surprisingly, DHS's release of draft federal chemical security regulations in December 2006 led to significant concerns from states with security regulations already in place for certain chemical facilities. Although preemption language was noticeably absent from Section 550 of the Department of Homeland Security Appropriations Act of 2007, the proposed rule was clear, stating: "No law, regulation, or administrative action of a State or political subdivision thereof, nor any decision or order 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."[1] It further stated that specific questions about preemption could be taken up with the Department. During the subsequent comment period, numerous parties voiced opinions both for and against preemption.

The interim final rule for federal chemical security regulations, released in early April 2007, noted consideration of public comments and explained the Department's view on preemption within its preamble. In sum, the Department asserted that "conflict preemption," rather than "field preemption," falls under Section 550 and that it intends to offer opinion on any issues of preemption in consultation with relevant States or local jurisdictions. However, DHS essentially kept the same language as previously proposed in § 27.405. As a result, states that previously implemented stringent standards for chemical facilities, such as New Jersey, may see those standards superseded by the new federal regulations once they come into effect on June 8, 2007.[2]

Despite DHS leadership holding to their assertion that the new regulations will likely not affect existing state laws, some members of Congress are taking steps to guarantee that state chemical regulations will be upheld. Using the emergency supplemental appropriations bills making their way through Congress, as well as individual bills, members proposed language to address the issue. One such bill, H.R. 1591, that primarily dealt with funding for the war in Iraq, was vetoed by the President on May 1, 2007. Congress is now seeking to approve a second funding bill for the war, H.R. 2206, which once again includes a provision on preemption. Members have also considered adding chemical security and preemption language to the 2008 homeland security appropriations bill. With these pieces of legislation currently pending, and the possibility of H.R. 2206 also being vetoed, members of Congress remain focused on the insertion of commensurate provisions in additional bills. ❖

[1] "Chemical Facility Anti-Terrorism Standards; Proposed Rule," Code of Federal Regulations, 6 § 27.405(a), December 28, 2006.

[2] Note: The list of "DHS Chemicals of Interest" does not fall under the June 8, 2007 effective date. A separate effective date will be announced following consideration of public comments.

Secretary Chertoff Addresses Chemical Security Regulations

On April 2, 2007, the Department of Homeland Security's Secretary Michael Chertoff, Under Secretary for National Protection and Programs Division George Foresman, and Assistant Secretary for Infrastructure Protection Bob Stephan provided a briefing and question/answer session on the interim final regulation for chemical security. Key sections of Secretary Chertoff's statement are highlighted in this article. Full text of the briefing is available at http://www.dhs.gov/xnews/releases/pr_1176131047481.shtm.

Secretary Chertoff: As you remember, last December, we released for comment a draft chemical security regulation, the general idea being we were going to have a risk-based regulatory framework for the chemical sector. Now, it's obviously very important to the economy that we have a chemical sector that is capable of functioning and being prosperous, but it's also true that we know that the aggregation or the collection of a lot of potentially dangerous chemicals in one place does create an attractive target to somebody who wants to carry out a terrorist attack.

We're not saying that there's any threat information about an imminent attack or a specific attack. We are saying that we know if we look at the history of how terrorists operate, they tend to try to leverage or exploit our own technology against us. And obviously, 9/11 was an example of that.

So for that reason, for some period of time, there's been a lot of public focus and discussion, as well as departmental focus about those areas where we have chemical industries or chemical storage facilities that house massive quantities of chemicals in proximity to high-density population centers. (...)

"Now let me say, this is not the only effort we have taken with respect to chemical regulation since 9/11. We began after 9/11, first of all by working with industry, and state and local governments to actually get out into the field and conduct vulnerability and threat assessments at hundreds of chemical sites across the country. This gave us a better understanding of what the actual risks were."

This regulation is going to impose for the first time, comprehensive federal security regulations for previously unregulated high-risk chemical facilities. It will go into effect in about 60 days – it's going to set national standards for chemical security, allowing us to create a risk-based, tiered structure for high-risk chemical plants, focusing, logically, on the most dangerous plants as those where the most demanding security requirements will be required by the regulation. (...)

Again, as I said in December, our approach is to work first with those facilities that present the highest risk, identify their weaknesses, and set forth some performance measures and security standards, which they will have to reach.

Now, what we do we mean by high-risk facilities? Well, we look at chemical plants and facilities and ask ourselves what kind – what is the kind and what is the quantity of chemicals that they have, because that's obviously a critical component of the threat that they pose. We look to see what the vulnerabilities are, and we look to see what the consequences would be of an explosion, for example, that dispersed a chemical cloud in a surrounding region. And that means we're particularly interested in the location that these plants are currently built in.

In fact, going beyond those specific plants we've identified, we are simultaneously releasing today a proposed list of chemicals of interest, which we're going to be seeking public comment on for the next 30 days. And what I mean by this is we are putting together a table of potentially dangerous chemicals and amounts, and telling the chemical industry that if you have housed on your facility chemicals in the quantities set forth, you are potentially in

(Continued on Page 10)

Chertoff *(Cont. from Page 9)*
the category of plants that may fall subject to regulation. And what you need to do in that instance is to go through the process of analyzing in what we call our top-screen process – it's an online analysis tool – you've got to go through that, and you've got to see whether, in fact, you meet certain criteria. We will then review that, and we will make a determination whether you fall within one of the four higher-risk categories.

I want to emphasize that this doesn't mean that every one of the plants that houses these chemicals will be deemed to be high risk. I mean, one could be, for example, literally in the middle of the desert, and that might make it comparatively low risk.

It does mean, though, we are going to be more comprehensive than we have ever been in making sure that we have a full picture of all the chemical-based risks that are out there, and making sure we are systematically driving down the risks in the most dangerous plants.

Finally, I want to emphasize that we are talking about performance-based measures and not micro-management from Washington. In other words, we want to set down standards and requirements, but we do not want to necessarily prescribe the exact way in which a plant is going to meet those standards or achieve those performance requirements. That's because we want to unleash the ingenuity of the private sector to figure out what is the best way to skin this cat, just as long as the cat gets skinned at the end of the day.

Now, let me take you through a little bit of the nuts and bolts about how this is going to happen, and then talk about a couple of issues, which I think you'll be particularly interested in. All plants, both those that we currently have on our list to notify and those that identify themselves through the table of chemicals we're going to be issuing, are going to be required to complete an on-line security assessment through a secure DHS website.

Part of this, by the way, is the fact that the more dangerous the chemical, the higher the risk tier. And that creates, certainly, an option for a lot of plants to decide they want to use – or change their operations to use lower-risk chemicals, which would bring them down in the level of tiers, and would thereby reduce the amount of regulatory or protective activity they have to undertake.

> "The bottom line is, our interest is in creating national standards and mandating a consistent responsible level of security, but not in interfering with the interests of states in making sure that they are taking the steps they feel are necessary to keep their citizens safe."

Now again, I want to emphasize, the fact that you complete the assessment doesn't mean you're going to be regulated, but that is the kind of baseline way of measuring the universe of people we need to worry about.

Facilities that we determine need to be regulated or need to do some further work are going to be contacted by the department. And then they will have 60 days to provide information for the department's risk-assessment process. We'll evaluate those submissions to determine which facilities have a preliminary high-level security risk, and those will be covered by the regulations.

We're also going to divide high-risk facilities into four tiers, and the higher up you go in the tiering, the more – the tougher, frankly, the security measures are going to be. And that's because the highest tier plants are going to be those where the greatest risk to the public is presented.

Our initial estimate is there could be as many as 7,000 facilities that will fall in the high-risk category in one of those four tiers. And we – again, we assess that there probably would be about 300 to 400 that will fall in the top two tiers. Once we actually get the risk assessments, we'll be a little bit more refined.

All of the high-risk facilities will have to prepare and submit vulnerability assessments and, more important, site security plans. And those are the plans we're going to evaluate for quality and for compliance with the performance standards. To manage this process, we're going to use our Chemical Security Compliance Division housed within the Office of Infrastructure and Protection, led by Bob Stephan. For fiscal year '08, we've requested $25 million to staff and support this new office.

Among the kinds of performance standards we're looking for are, standards about how long and how
(Continued on Page 13)

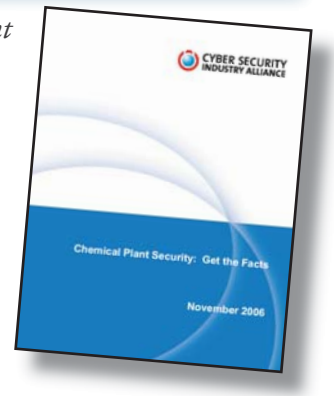
Cyber Security Industry Alliance's Report on Chemical Plant Security

The Cyber Security Industry Alliance (CSIA) released a report "Chemical Plant Security: Get the Facts" in November of 2006. This report discusses the importance of the chemical sector to the U.S. economy, the cyber threats to the chemical sector and the new legislation. In the report, CSIA explains why cyber security is critical to the chemical sector:

> *Physical threats aside, the chemical sector - and much of the nation's critical infrastructure - functions on control systems, which are electronic, software-based systems that monitor and control the functions and processes of the plants. Establishing and implementing minimum cyber security standards in order to protect our chemical plants from system failures, intrusions or terrorist attacks is crucial to the viability of our overall critical infrastructure.*

CSIA further succinctly sums up their position on the cyber security issues faced by the chemical sector in the following section:

> *CSIA believes that stronger cyber protection is needed to secure the chemical sector and that closer cooperation is needed between the private sector and agencies responsible for certifying information security products purchased by the federal government. While some progress has been made, much work remains to properly secure the chemical sector's critical infrastructure. CSIA urges President Bush to form a task force of key government agencies, appropriate regulators, experts in the cyber security field and representatives from not only the chemical sector, but also other utilities and suppliers, to meet and recommend concrete actions to improve the security of control systems supporting critical infrastructure.*



The full report is available at https://www.csialliance.org/publications/csia_whitepapers/CSIA_Chemical_Plant_Security_Get_Facts_November_2006.pdf ❖

Chemical Sector Coordinating Council

The Chemical Sector Coordinating Council is recognized by the Department of Homeland Security, numerous federal agencies, and other sector coordinating councils as the primary focal point of activities and information dissemination related to chemical security. The Coordinating Council acts as a representative between the government and other critical infrastructure sectors to convey the sector's security priorities and input into policy decisions.

Current membership of the Chemical Sector Coordinating Council includes:

American Chemistry Council
American Forest & Paper Association
Chemical Producers and Distributors Association
Chlorine Chemistry Council
Compressed Gas Association
CropLifeAmerica
Institute of Makers of Explosives
International Institute of Ammonia Refrigeration
National Association of Chemical Distributors
National Paint & Coatings Association
National Petrochemical & Refiners Association
Synthetic Organic Chemical Manufacturers Association
The Adhesive and Sealant Council
The Chlorine Institute
The Fertilizer Institute
The Society of the Plastics Industry, Inc.

Higher Education Responds to Chemical Regulations

The new chemical regulations do not only affect chemical facilities. As noted in the following excerpts from a letter by the American Council on Education (ACE) and the National Association of College and University Business Officers (NACUBO), the standards have implications for thousands of research institutions as well.

Summary of Comments

The Interim Final Regulation imposes a multi-step process intended to give DHS information it needs to determine which chemical facilities present what level of risk from terrorist concerns. Based on that information, DHS would phase in requirements to perform facility assessments and prepare site security plans to address and prevent those risks. This phased in effort would require that those entities facing the greatest risk take action first. However, the first step in the process requires that every entity that might possibly possess or plan to possess any of 342 substances, complete what is called a "Top-Screen" analysis. To complete that analysis the entity must first inspect its operations to see which of the 342 chemicals are present, and in what amounts. If even one of 104 specified chemicals is present in even the smallest amount, the Top-Screen must be fully completed.

Colleges and universities have hundreds if not thousands of laboratories and classrooms that may well contain miniscule amounts of one or more of the substances listed in Appendix A (6 C.F.R. 27). In order to complete the Top-Screen analysis, each college, university, community college and other institution of higher education must inspect every building, laboratory and classroom where any science course is taught, to determine which one might contain just one of these substances. Even after this effort, it is almost certain that not a single college or university will be found to be a chemical facility that presents a high risk of terrorist attack. We urge the DHS not to divert its resources from the important task of ensuring that chemical facilities are protected, by converting a program intended to regulate chemical facilities into a program to regulate any facility where miniscule amounts of a single chemical might exist. Instead, DHS should phase in Appendix A by providing that it will not be effective as to the higher education sector until such time as it we can meet with DHS and provide specific suggestions to make its applicability more relevant and effective.

"Colleges and universities have hundreds if not thousands of laboratories and classrooms that may well contain miniscule amounts of one or more of the substances listed in Appendix A..."

The higher education community recognizes the enormous challenge DHS faces in protecting the nation against chemical-based attacks. DHS must develop and implement a program to address the potential for a terrorist attack aimed at targets having chemical substances that, if released, could cause enormous injury and damage. Although it took four years for Congress to enact legislation authorizing this program, DHS is required to implement it in 180 days. Moreover, DHS must accomplish this task, yet not undermine or compromise the dozens of other federal, state and local efforts already in place or under way to address similar concerns. At the same time, it is the private businesses and organizations, including the higher education sector that are faced with the obligation to undertake reviews and create and implement plans to achieve these legislative ends. It is in this spirit that we offer the following comments to Appendix A and the Interim Final Regulations.

1. It is inappropriate and unnecessary to require higher education institutions to search thousands of small laboratories for the presence of any of the 342 substances listed on Appendix A.

2. Appendix A should be modified to correct technical errors and to comport with threshold quantities established by existing

(Continued on Page 15)

"We're obviously concerned that someone attacking and exploding such a facility or stealing from such a facility could pose a hazard to human life in a dense urban area, and that's something that we want to be very focused upon."

Chertoff *(Cont. from Page 10)*
robustly you secure the perimeter and the critical target, how you control your access, how you deter and prevent theft of potentially dangerous chemicals, and how you prevent internal sabotage. And of course, we want to provide guidance at every step of the way to the chemical industry in terms of the various ways they might meet these objectives.

Finally, we will be using site inspections and audits to ensure that those performance-based standards that have been imposed will, in fact, be implemented.

Critical to this is partnership, partnership with the chemical industry. Where a vulnerability assessment or a site security plan does not meet our approval, the facility is going to need to revise the plan and resubmit it. But for our part, we're going to provide technical assistance to help those plants get to the place they need to be.

And the final point I want to make is accountability. Facilities that, after we give it a good college try, fail to meet our performance standards could face penalties of up to $25,000 for each day during which a violation occurs, or they could be ordered to halt operations until security is brought up to a level we feel is appropriate. Now, I'm confident that most chemical plants will voluntarily accomplish what we need to get done in the area of security. Many of them probably already have standards that are sufficient. But the important thing is to make sure that we bring even those that are laggard into compliance with what the public has a right to expect five years after September 11th.

Let me talk about one last issue, which is, what is, in particular, different about this rule, as compared to the rule we issued in December? I think there are four differences. One is, last December, we had not published a list of chemicals. This regulation is going to be accompanied by a proposed list of chemicals, which will guarantee that we are comprehensively reaching all of the facilities that ought to be in the universe subject to this rule.

Second, we have clarified the fact that confidential chemical terrorism vulnerability information will be shared with appropriate state and local officials, including, importantly, police and first responders. This is designed to clarify a misconception that somehow we were not going to let the cops and firefighters in the vicinity know what was going on at a chemical plant. Quite the opposite. It's very important that we get local authorities very tightly bound in with our process.

Third, is that we have determined that although a lot of plants have done their own site assessments for the three highest tiers, we will require them to submit those assessments using the particular on-line assessment tool that we're going to be providing in our secure website. We recognize a lot of work has been done on assessments already. It shouldn't be particularly onerous to configure those into the assessment tool that we're providing. I liken it to what you do around tax time, which is, you collect all your financial material, but you need to get your account actually fitted into the form 1040.

But we do need to make sure that we're operating off the same sheet of music in terms of understanding what the vulnerabilities are and what the security plans are.

Finally, let me get to the issue of preemption. Perhaps more than any other element of the regulations in December, the question of federal preemption of state law occupied a great deal of public attention and some public controversy. Let me begin by saying that some states, although not many, have existing laws for regulating chemical facilities with respect to chemical security. What we are concerned about in terms of preemption are only state laws and requirements that would conflict or interfere with the federal regulations, and only those would be preempted. Currently, the department has no reason to conclude that any of the existing state laws and regulations that are out there, dealing with chemical security, are being applied in a way that would impede or interfere with the federal rule. (...)

Before I conclude, I want to emphasize the vital role that state and local
(*Continued on Page 15)*

Interim Rule Standards *(Cont. from Page 4)*

(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;
(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
(10) Monitoring. Maintain effective monitoring, communications and warning systems.
(11) Training. Ensure proper security training, exercises, and drills of facility personnel;
(12) Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets.
(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;
(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;
(16) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
(17) Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards;
(18) Records. Maintain appropriate records; and
(19) Address any additional performance standards the Assistant Secretary may specify. ❖

Legal Insights *(Cont. from Page 6)*

tions certain State and local officials may possess a need to know, but DHS has sole discretion to make that determination. At the same time, persons with a need to know may require security background checks and are subject to strict confidentiality requirements. Also, DHS has asserted that any information shared by the Agency will be protected from state "sunshine" or "right-to-know" laws and that these State laws are deemed to be preempted.

Outside experts have long criticized homeland security information sharing efforts between the federal, state and local government agencies. In the maritime sector, GAO has documented a long and difficult process of information sharing that has only recently improved after five years and continues to be hampered by security clearance delays for state and local first responders. But while MTSA rightly protects classified and sensitive port security information from public disclosure, MTSA also provides important mechanisms for information sharing that are not included in the Chemical Security Rule. These mechanisms—Area Maritime Security Committees and Interagency Operation Centers—include key port stakeholders and have greatly enhanced coordination and improved information sharing leading to better overall security according to GAO.

With the creation of a complex new information protection regime covering the chemical sector, it is difficult to see how effective information sharing in the chemical sector between first-responder agencies can be accomplished without enormous expenditures of time and resources. ❖

ACE Letter *(Cont. from Page 12)*

programs.

3. Proposed Appendix A amplifies the ambiguities faced by colleges and universities who attempt to comply with the new rules.

4. The consultation offered by DHS to assist in answering these difficult questions is unlikely to resolve these serious concerns.

5. Appendix A may expose college and university officials to serious criminal sanctions if they fail to complete the Top-Screen to the satisfaction of DHS.

6. DHS should exempt colleges and universities from the Top-Screen requirement.

The full letter sent by ACE to the Department of Homeland Security can be found at http://www.acenet.edu/AM/Template.cfm?Section=HENA&Template=/CM/ContentDisplay.cfm&ContentID=22162. ❖

Chertoff *(Cont. from Page 13)*

authorities play in protecting our country. Chemical security is not a federal responsibility, it is a shared responsibility, and not just among federal, state and local governments, also with the private sector, as well.

We all have to work together to implement the best possible measures to strengthen the security of our chemical facilities while not undercutting what is a very important element of our national economy.

The rule we've announced today is a culmination of a lot of back and forth, a lot of input. We have listened, and where we feel that points had merit, we've adopted those points. We now look forward to working with the industry and with state and local government to implement this rule, and to move quickly to strengthen protection of this vital part of our economy. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1