NEW JERSEY LAWYER
Magazine
October 2007 / No. 248

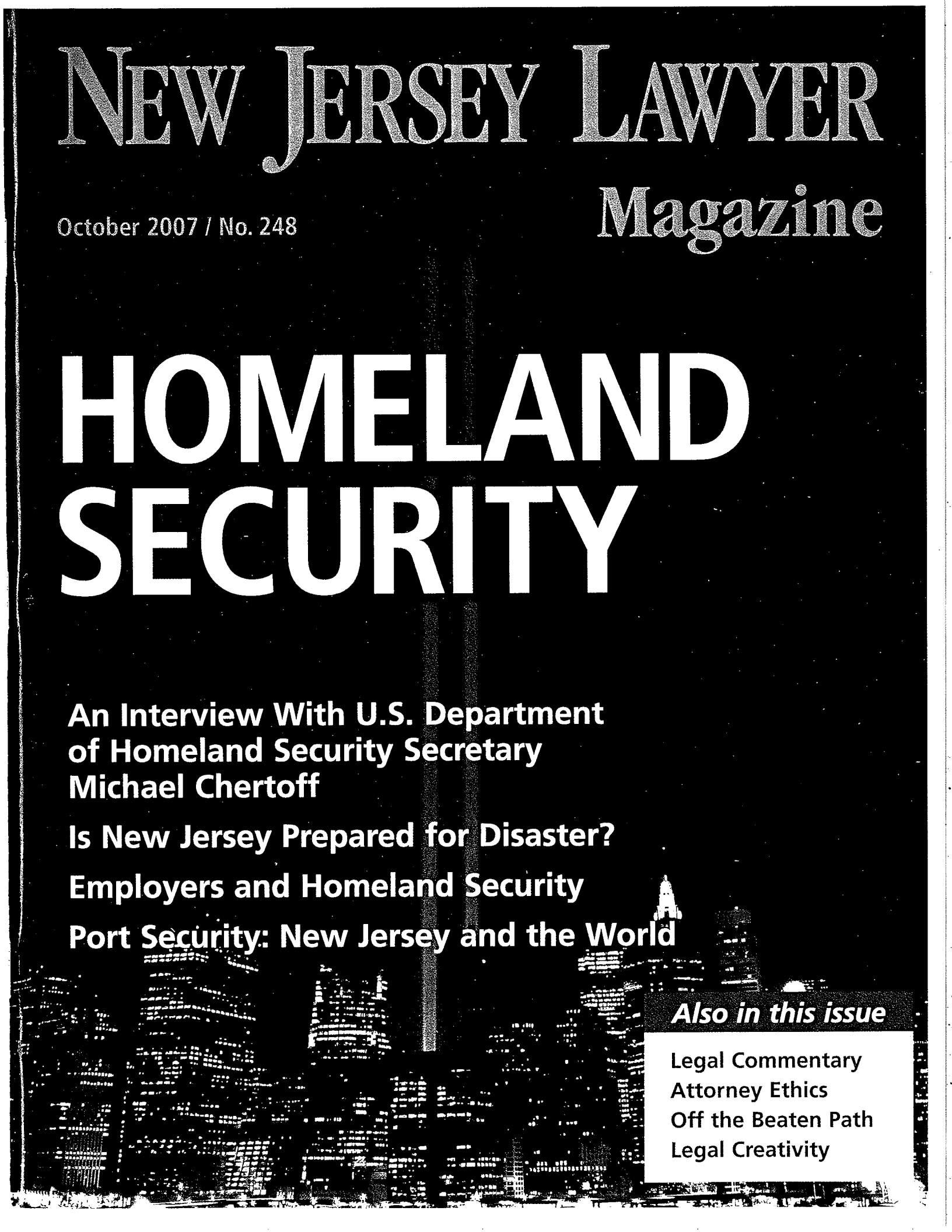
# HOMELAND SECURITY

An Interview With U.S. Department of Homeland Security Secretary Michael Chertoff

Is New Jersey Prepared for Disaster?

Employers and Homeland Security

Port Security: New Jersey and the World



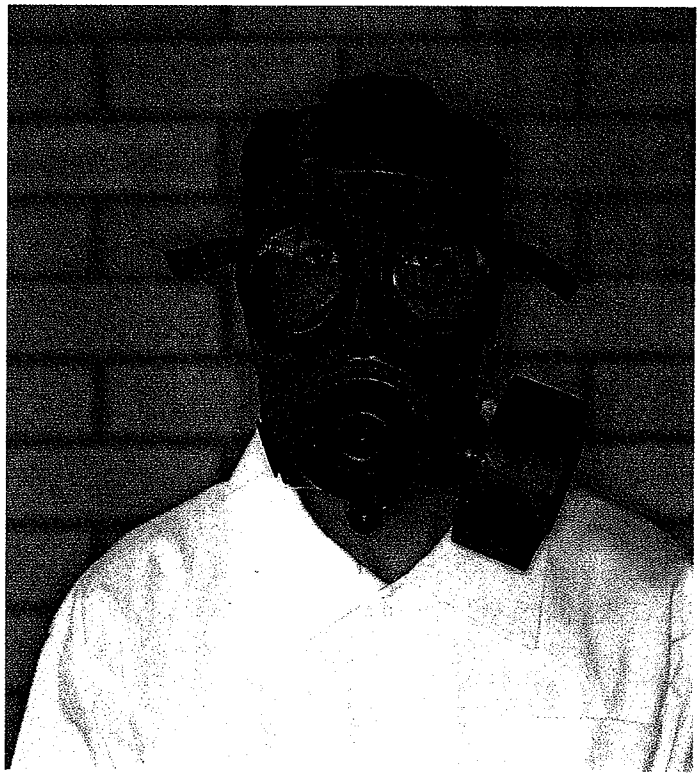
*Also in this issue*

# Chemical Security: Recent Regulations and the Impact on the Private Sector

**by Joe D. Whitley and George A. Koenig**

There are thousands of chemical facilities in the United States. Although only a small fraction of the nation's chemical facilities represent the high-risk targets that worry homeland security officials most, a terrorist attack against any one of them would be a significant national event, and could result in the loss of life. It is for this reason that safeguarding chemical facilities remains a homeland security priority, and Congress statutorily mandated that the Department of Homeland Security (DHS) promulgate regulations for chemical facility security by April 2007.[1] Although these regulations directly affect the chemical industry, they likely are a template of what's to come for other industries, as the private sector enters a new area of homeland security oversight.

Chemical facilities are part of the nation's overall critical infrastructure. Congress defines critical infrastructures as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[2] More simply put, critical infrastructures are the processes that enable 21st century life. In addition to chemical facilities, power plants, transportation nodes, financial networks and communications systems are also critical infrastructures. In many cases, they are interdependent, and a substantial decrease in capacity in one critical infrastructure sector may have a catastrophic ripple effect regionally or nationally.



Although Sept. 11, 2001, heightened the importance of critical infrastructure protection, efforts to safeguard them are more than a decade old. After the 1993 World Trade Center attack and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the Clinton Administration

began to address critical infrastructure protection.[3] These efforts continued under the Bush Administration.

Following Sept. 11, the White House authored Homeland Security Presidential Directive 7 (HSPD-7). HSPD-7 establishes the U.S. policy for "identify[ing] and prioritiz[ing] United States critical infrastructure and key resources...," and mandates a national plan to achieve that policy.[4]

Pursuant to the requirements of HSPD-7, DHS released the National Infrastructure Protection Plan (NIPP) on June 30, 2006. The NIPP underscores the importance of protecting critical infrastructures and establishes the goal of:

> [b]uild[ing] a safer, more secure, and more resilient America by enhancing protection of the Nation's [critical infrastructures] to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.[5]

The NIPP creates the framework for unifying critical infrastructure protection efforts across the nation, and seeks to mitigate risk by deterring threats, reducing vulnerabilities and minimizing consequences associated with a terrorist attack or other incident.[6] Because the private sector controls 85 percent of the nation's critical infrastructure, industry's voluntary participation in the NIPP's risk management process is critical.[7]

As previously noted, critical infrastructures may be defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[8] Specifically, there are 12 critical infrastructure sectors in the United States:

- Defense Industrial Base
- Food and Agriculture
- Public Health and Healthcare
- Postage and Shipping
- Energy
- Transportation Systems
- Banking and Finance
- Information Technology
- Telecommunications
- Drinking Water and Water Treatment Systems
- Chemicals and Chemical Facilities[9]

For important sites/resources either not classified directly as a critical infrastructure or for which additional security considerations must be addressed, there are five categories of key assets:

- National Monuments and Icons
- Commercial Nuclear Reactors, Materials and Waste
- Dams
- Emergency Services
- Commercial Facilities (such as prominent commercial buildings, hotels and sports stadiums)[10]

## Why the Chemical Sector?

Data compiled by the American Chemistry Council (ACC) show that the U.S. chemical industry is among the nation's most important commercial sectors, representing more than six percent of U.S. manufacturing jobs and comprising more than 15,000 chemical facilities.[11] The entire chemical supply chain includes not only chemical facilities but also the rail networks, ships, and trucks that transport chemicals domestically and for export. The intermodal nature of the chemical industry requires a dynamic approach to security that leverages the best practices and expertise of industry, government, and international partners.

Threat briefings provided by the government's most senior law enforcement and intelligence officials showcase the ongoing concern: Terrorists continue to seek weapons of mass destruction, including chemical agents. In a recent statement before the Senate Select Committee on Intelligence, Federal Bureau of Investigation Director Robert Mueller told the panel that "...if it can, al-Qa'ida will obtain and use some form of chemical, biological, radiological or nuclear (CBRN) material."[12] Targeting a chemical facility is one way to achieve this goal, and eliminates the need for a terrorist to physically produce a chemical or a mechanism to disperse it.

Despite sometimes dire predictions, the suggestion that the chemical industry (and individual chemical companies) failed to take steps to harden the most vulnerable sites is inaccurate. ACC launched a series of initiatives following Sept. 11 to enhance chemical facility security. As the leading trade organization, the ACC counts America's largest chemical companies among its ranks and used its influence to raise awareness and develop security best practices.

ACC's Responsible Care Security Code Program represents "...an aggressive plan to further enhance security of our facilities, our communities and our products."[13] While the security code improved security at many chemical facilities, the fencing, cameras, vehicle barriers, and other security enhancements varied from facility to facility. For those that did not participate in the security code program, improved security came late, if at all. Other chemical facilities continued to view security as a cost center with few positive externalities, and undertook few security improvements after Sept. 11.

For these reasons among others, Congress renewed its efforts to create national, uniform chemical facility security standards. Congress held several hearings during the summer of 2005. The

conclusion of these hearings was straightforward: A voluntary chemical security program was insufficient. The nation needed the force of law to ensure that the most at-risk locations implemented safeguards commensurate with the risk. Echoing the sentiment of many, Assistant Secretary for Infrastructure Protection Bob Stephan told a Senate panel that "...it has become clear that the entirely voluntary efforts...alone will not sufficiently address security for the entire [chemical] sector."[14]

By the end of 2005, at least one bipartisan proposal, the Chemical Facility Anti-Terrorism Act of 2005 (S.2145) gained momentum. It was Section 550 of the Department of Homeland Security Appropriations Act of 2007, however, that gave DHS the statutory authority to regulate chemical facilities.[15] A mere two pages, Section 550 provided scant guidance to DHS, and the department was left to its discretion to create implementing regulations to effectuate what congressional intent could be gleaned from the statute itself. Despite its brevity, Section 550 offers a legal framework and overarching policy goals to guide the creation of implementing regulations.

First, Section 550 requires DHS to create "risk-based performance standards." Unlike a traditional regulation that mandates *how* to achieve a desired result, a performance standard requires a certain outcome but not the precise manner to achieve it. In other words, so long as the end is achieved, the means is immaterial. There is rarely a one-size-fits-all solution to a security challenge, and the use of performance standards permits chemical facilities to select the most appropriate security measure to achieve the desired outcome. Consistent with performance-based standards, DHS cannot approve or disapprove a security plan based on the presence or absence of a specific security measure.

Additionally, the performance standard is risk-based; those facilities that present the greatest harm require the greatest level of security. A chemical facility near a populated urban area presents a greater risk than a similar facility in a sparsely populated area. Security measures must be implemented accordingly.

Many chemical facilities have increased security aggressively since Sept. 11, even in the absence of a compulsory reason to do so. In some instances, a chemical facility may be entitled to use its current security measures to satisfy the Interim Final Rule on Chemical Facility Anti-Terrorism Standards (CFATS).[16] The use of an alternative security plan in this context must satisfy the applicable risk-based performance standard. Importantly, while Section 550 grants DHS the statutory authority to regulate the chemical sector, it has a three-year sunset provision and will need to be reauthorized either by this Congress or the 111th Congress.

## The Chemical Facility Anti-Terrorism Standards

Following a brief notice and comment period, DHS published CFATS on April 9, 2007. Other than Appendix A (discussed below), CFATS took effect on June 8, 2007, and establishes risk-based performance standards for the security of high-risk chemical facilities.[17] Chemical facilities that meet the threshold requirements of Appendix A, or are otherwise identified by DHS as potentially high-risk,[18] must complete a questionnaire known as the top-screen. The questionnaire elicits information to help DHS determine whether a chemical facility will be covered as high-risk and, therefore, regulated. As such, it will be referred to as a "covered facility," which CFATS defines as "...a chemical facility determined by the Assistant Secretary to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk...."[19]

Depending upon the perceived risk, covered facilities will be placed in one of four risk tiers with commensurate security obligations. DHS will provide the general tier criteria to covered facilities through forthcoming guidance documents, but the actual determination allocating a covered facility to a tier will be protected information. Covered facilities will be required to prepare security vulnerability assessments (SVAs) and site security plans (SSPs) that must be approved by DHS. In short, the SVA identifies facility security vulnerabilities. The SSP includes measures that satisfy the identified risk-based performance standards.

CFATS also contains provisions concerning inspections, audits, recordkeeping and the protection of sensitive chemical terrorism vulnerability information. It also provides DHS with the authority to assess fines and, in extreme cases, issue an order for the cessation of operations.

CFATS describes a regulatory agenda divided among several steps:

- **Chemical Facility:** DHS defines chemical facility as "any establishment 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."[20]
- **Exemptions:** Pursuant to Section 550, Congress statutorily exempts five types of facilities:
  - facilities regulated by the Maritime Transportation Security Act of 2002;
  - Public water systems, under Section 1401 of the Safe Drinking Water Act;
  - Treatment works, under Section 212 of the Federal Water Pollution Control Act;
  - Any facility owned or operated by the Department of Defense or Department of Energy; and
  - Any facility regulated by the Nuclear Regulatory Commission.

- **Implementation:** DHS will implement this regulatory program in phases.[21] A coordinating official will be appointed "who will be responsible for ensuring that these regulations are implemented in a uniform, impartial, and fair manner." The coordinating official and his or her staff will provide guidance to facilities regarding compliance; resources permitting, the coordinating official also will provide consultation and technical assistance to covered facilities.[22]
- **Initial Screening:** DHS would require non-exempted chemical facilities that *may present* "high levels of security risk" to complete the top-screen risk assessment,[23] which is one part of an overall process of collecting data under the chemical security assessment tool (CSAT).[24]
- **Selection for Top-screen:** The presence or amount of chemicals listed in Appendix A will serve as a baseline threshold to require a facility to complete the top-screen.[25] However, DHS has been careful to say that the "presence or amount of a particular chemical listed in Appendix A is not the *sole factor* in determining whether a facility presents a high-level of security risk, and is *not an indicator* of a facility's coverage under this rule."[26] DHS also may notify facilities—either directly or through a *Federal Register* notice—that they need to complete and submit a CSAT top-screen.[27] Facilities that meet the threshold baseline will have 60 calendar days to complete the top-screen from the effective date of publication of the final Appendix A.[28]
- **Top-screen Questions:** The questions presented by the top-screen will solicit broad information related to security and emergency preparedness issues, and may include questions such as the "nature of the business and activities conducted at the facility; the names, nature, conditions of storage, quantities, volumes, properties, customers, major uses, and other pertinent information about specific chemicals or chemicals meeting a specific criteria; information concerning facilities' security, safety, and emergency response practices, operations and procedures; information regarding incidents, history, funding, and other matters bearing on the effectiveness of the security and response programs, and other information as necessary."[29]
- **Submission of Top-screen:** Chemical facilities would submit top-screen results via a secure Web portal or through other means approved by DHS.[30]
- **Presumption of High Risk:** Chemical facilities that are required or ordered to provide information or complete the top-screen—but fail to do so in a timely manner—may be classified as presumptively high risk, and be subject to civil penalties and ordered to cease operations.[31]
- **Non-High-Risk Facilities:** If, after reviewing the top-screen results, DHS determines that a particular chemical facility does not present a high level of security risk, then DHS would notify the chemical facility of this finding. The chemical facility would have no further regulatory obligation under CFATS.[32]
- **Covered Facilities:** If, after considering those factors, DHS determines that a chemical facility does present a high level of security risk, then DHS would notify the chemical facility of this finding, and also may notify the facility of its preliminary placement in a risk-based tier (highest Tier 1 to lowest Tier 4). These covered facilities would be required to take additional steps pursuant to the CSAT. The covered facility must complete and submit an SVA and an SSP within 90 days and 120 days, respectively, of written notification from DHS or *Federal Register* notice.[33] According to the DHS website "Covered facilities contacted by the department will have 120 days from the publication of the regulation in the *Federal Register* to provide information for the risk assessment process. Other requirements follow that time period. Additional facilities will follow a similar timeframe after future *Federal Register* publications."[34]
- **Resubmissions:** Tier 1 and Tier 2 covered facilities must resubmit a new top-screen every two years. Tier 3 and Tier 4 covered facilities must resubmit a new top-screen every three years. Upon resubmission of the top-screen, covered facilities are also required to resubmit SVAs and SSPs within 90 and 120 days, respectively.[35] Facilities also may have to make a resubmission if there has been a "material modification."
- **Security Vulnerability Assessment:** An SVA evaluates risk by considering diverse factors. An SVA includes features such as asset characterization, threat assessment, security vulnerability analysis, risk assessment, and countermeasure analysis. In the proposed rule, DHS had emphasized the risk analysis and management for critical asset protection (RAMCAP) vulnerability assessment methodology to complete the vulnerability assessment, though alternative vulnerability assessment methodologies (*e.g.*, alternative security programs as discussed below) may satisfy the requirement.[36] Under CFATS, DHS has decided to employ a modified version of RAMCAP (*i.e.* CSAT) and, with limited, exception has made CSAT the preferred methodology.[37]
- **Tiers:** Upon review of information it receives, including top-screen submissions, DHS will make a preliminary decision regarding placement of each covered facility in a risk tier. The risk tier will include covered facilities

with similar risk profiles. DHS has identified four tiers, with Tier 1 representing the highest-risk facilities. DHS will confirm or alter its preliminary tier decision after reviewing a covered facility's SVA. The assigned tier will determine which risk-based performance standards apply.[38]

- **Site Security Plan:** The SSP is a security and emergency preparedness roadmap. Specifically, the SSP must remediate deficiencies identified by the vulnerability assessment and satisfy the applicable risk-based performance standard. Because a performance standard, by definition, seeks a specific result or outcome but does not direct the *manner* or *means* to achieve it, precise security measures are not mandated. For example, DHS can mandate that all Tier 1 facilities achieve a required *level* of protection (*i.e.*, meet the risk-based performance standard). DHS cannot mandate that all Tier 1 facilities install specific vehicle barricades or perimeter intrusion detection systems to do so. Accordingly, DHS cannot disapprove a SSP based on the presence or absence of a specific security measure. DHS can only disapprove a SSP if the plan, as a whole, fails to satisfy the applicable risk-based performance standard.[39]
- **Alternative Security Program (ASP):** As noted, many covered facilities have enhanced their security voluntarily since Sept. 11. Robust security vulnerability assessments, site security plans, and other preexisting emergency initiatives have resulted in a level of preparedness that, in some cases, meets or exceeds CFATS. Recognizing the progress that has already been made, DHS may accept an ASP as a substitute for some of the mandates proposed by this regulatory scheme. An approved ASP must provide an equivalent level of security as would the requirements of CFATS. Depending upon a covered facility's tier, CFATS permits submission of an ASP for DHS approval in lieu of an SVA or SSP, or both. DHS will *not* accept an ASP in lieu of an SVA for Tiers 1-3 (higher risk facilities), but may accept an ASP as substitute for an SSP for Tiers 1-3. Tier 4—the lowest risk facilities—may submit an ASP rather than an SVA, SSP, or both.[40] DHS explains its rationale for these distinctions.[41]
- **Approvals:** DHS must review and approve all SVAs, SSPs and ASPs. If any submission is deemed inadequate, DHS will notify the covered facility of the deficiencies and provide a deadline for resubmission.[42]
- **Material Modifications to Operations or Site:** Because threats, vulnerabilities, and consequences change, covered facilities have an affirmative obligation to amend and resubmit SVAs and SSPs as situations warrant, or as required by DHS. A facility will have 60 days from the date of the "material modification" to make its resubmission.[43]
- **Audits and Inspections:** Following initial approval of a site security plan, DHS proposes to ensure compliance through audits and inspections. These audits and inspections will be conducted at a "reasonable time" and in a "reasonable manner," and typically with 24 hours notice. However, in exigent circumstances, DHS may conduct unannounced inspections. DHS will be issuing more guidance regarding inspections.[44] DHS will use its own auditors and inspectors to inspect high-risk tier facilities, and DHS will be issuing a future rulemaking about how it plans to use third-party auditors.[45]
- **Recordkeeping:** Covered facilities are required to maintain records related to security and emergency preparedness for *three years* (*e.g.*, training, drills and exercises; incidents and breaches of security; maintenance records regarding security equipment; audits; letters of authorization and approval).[46]
- **Orders and Adjudications:** If facilities are found in violation, DHS may assess fines (up to $25,000 per day) or require the cessation of operations.[47] A covered facility has a right to seek administrative review of such determinations. DHS will bear the initial burden of proving the facts supporting the administrative action in dispute.[48]
- **Chemical-terrorism Vulnerability Information:** Chemical facility security information (CVI)—such as SVAs, SSPs, alternative security programs and inspections and audits—is sensitive. It may be characterized not only as national security information but also as proprietary and confidential business information. Current law protects both from unauthorized disclosure.[49] Because of the security concerns regarding the types of information developed, maintained, and submitted in compliance with this new regulation, DHS has developed a new form of protected information. Only individuals with a need to know will have access to or otherwise obtain chemical-terrorism vulnerability information (CVI). CVI is intended to protect the most sensitive information exchanged between DHS and covered facilities, including documentation regarding: 1) SVAs; 2) SSPs; 3) DHS's review or approval of SVAs or SSPs; 4) alternate security programs; 5) inspections or audits; 6) recordkeeping requirements; 7) sensitive portions of orders, notices or letters; 8) top-screen or other similar documents related to tier determination; and 9) other sensitive information. CVI has specific access, marking, handling, and destruction requirements; CVI disclosure is further limited in administrative and judicial proceedings.[50]

- **Preemption:** While Section 550 of the Homeland Security Appropriations Act does not contain an express preemption provision, well-established principles of federalism preempt state or local laws that conflict with or frustrate the purpose of DHS's proposed regulatory scheme. DHS proposes to permit any covered facility or any state to "petition the Department by submitting a copy of a State law, regulation, or administrative action, or decision or order..." for a DHS-authored preemption opinion.[51]
- **Third-Party Actions:** Only the secretary has a right of action. There is no private right of action.[52]

## Ongoing Congressional Interest in Chemical Security Regulation and Proposed Changes to Section 550—Preemption

Some members of Congress are already considering making changes to Section 550. On March 27, 2007, DHS Secretary Michael Chertoff wrote Senator Robert C. Byrd about the war supplemental bills pending at that time in both houses that contained language affecting Section 550. Although President Bush vetoed the first war supplemental, and the war supplement bill approved by the president did not contain any amending language,[53] it is likely that changes to Section 550 will continue to be discussed, and may be included in future legislation. DHS appropriations language under consideration for 2008, for example, may permit state and local governments to enact chemical security rules that are more stringent than those required by CFATS. Preemption is a particularly important issue for New Jersey, and one that has been actively followed and commented on by Governor Jon Corzine and members of New Jersey's congressional delegation.

## Conclusion

Because CFATS may become the standard for future security regulation in other industries and critical infrastructures, corporate leaders—regardless of their core business—should monitor its implementation closely. It is conceivable that Congress will begin regulating other high-consequence and high-vulnerability industries in the near future. Learning lessons from the chemical industry's experience with security regulation may save companies time and money if and when regulation expands to other industries. ⚖

## Endnotes

1. Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, 120 Stat. 1355 (2006).
2. 42 U.S.C. § 5195c(e).
3. *See generally* The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructure (1997); *see also* Presidential Decision Directive/NSC-63 (May 22, 1998) *available at* www.fas.org/irp/offdocs/pdd/pdd-63.htm.
4. The White House, Homeland Security Presidential Directive/HSPD-7 (December 17, 2003) *available at* http://www.fas.org/irp/offdocs/nspd//hspd-7.html.
5. The U.S. Department of Homeland Security, National Infrastructure Protection Plan 1 (2006), *available at* www.dhs.gov/nipp.
6. *Id.*
7. Matthew E. Berger, *DHS, Private Sector Teamwork Required to Implement Infrastructure 'Playbook'*, CONG. Q., June 30, 2006, *available at* http://homeland.cq.com/hs/display.do?docid=2319613&sourcetype=31&binderName=news-all; *also see* 2006 WLNR 11605895 (Westlaw).
8. *Supra* note 2.
9. *Supra* note 5 at 3.
10. *Id.*
11. *See* http://www.americanchemistry.com/s_acc/bin.asp?CID=473&DID=1596&DOC=FILE.PDF
12. Current and Projected National Security Threats Before the Senate Select Comm. on Intelligence, 110th Cong. Sess. 1 (2007) (statement of Robert Mueller, Director of the Federal Bureau of Investigation).
13. *See* www.americanchemistry.com/s_responsiblecare/doc.asp?CID=1298&DID=5085
14. *Is the Federal Government Doing Enough to Secure Chemical Facilities and Is More Authority Needed? Before the U.S. Senate Committee and Homeland Security and Governmental Affairs*, 109th Cong. Sess. 1 (2005) (statement of Robert Stephan, Assistant Secretary for Infrastructure Protection, U.S. Department of Homeland Security).
15. *Supra* note 1 at § 550.
16. Chemical Facility Anti-Terrorism Standards; Final Rule 72 Fed. R. 17688 (April 9, 2007) (to be codified at 6 CFR Part 27). All terms shall have the meaning as defined herein or as contained in the CFATS.
17. As with most regulations, in order to understand CFATS, it is essential to know the meaning of certain key terms. Key definitions in CFATS can be found at §27.105. *Id.* at 17730.
18. DHS may determine at any time that a chemical facility presents a high level of security risk based on any information that, in the secretary's *discretion,* indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health, national security or critical economic assets. *Id.* at 17731. (§27.205).
19. *Id.* at 17730 (§27.105).
20. *Id.* at 17730. (§27.105).
21. *Id.* at 17730. (§27.115).
22. *Id.* (§27.120).

23. *Id.* (§27.105). Top-screen "is an initial screening process designed by the Assistant Secretary [for Infrastructure Protection] through which chemical facilities provide information to the Department...."
24. According to the CFATS, CSAT it is a suite of four applications, including user registration, top-screen, security vulnerability assessment and site security plan, through which DHS collects and analyzes key data from chemical facilities. *Id.* (§27.105) On April 25, 2007, DHS encouraged facilities that *think* they may be covered by CFATS to begin completing the applicable portions of the CSAT early to avoid potential delays or other unforeseen impediments. *See* Notice to Facilities to Begin Registration for Chemical Security Assessment Tool, 72 *Fed. Reg.* 20423 (Apr. 25, 2007).
25. *Id.* at 17731. (§27.200).
26. *Id.* at 17696.
27. *Id.* at 17731. (§27.200).
28. *Id.* (§27.210).
29. *Id.* at 17731. (§27.200).
30. *Id.* (§27.200).
31. *Id.*
32. *Id.*
33. The 90- and 120-day deadlines may be shortened or extended, if appropriate. *Id.* at 17731. (§27.210).
34. *See* www.dhs.gov/xnews/releases/pr_1175527925540.shtm.
35. *Id.* (§27.200).
36. DHS describes RAMCAP as "an overall strategy and methodology to allow for a more consistent and systematic analysis of the terrorist threat and vulnerabilities against the U.S. infrastructure using a risk-based framework." *Id.* at 78,303. As such, RAMCAP is a technical, engineering-based application requiring subject matters expertise. DHS provided a detailed RAMCAP overview in Appendix B to the proposed regulation.
37. CFATS at 17691.
38. *Id.* at 17732. (§27.220).
39. *Id.* at 17734. (§27.245).
40. *Id.* at 17733. (§27.235).
41. *Id.* at 17692-3.
42. *Id.* at 17734. (§§ 27.240 & 27.245).
43. *Id.* at 17732. (§27.210). DHS admits that it is difficult to provide an "exhaustive list" of what constitutes a "material modification," but expects that it would include changes at a facility to chemical holdings (including the presence of a new chemical, increased amount of an existing chemical or the modified use of a given chemical) or to site physical configuration that may 1) substantially increase the level of consequence should a terrorist attack or incident occur; 2) substantially increase a facility's vulnerabilities from those identified in the facility's SVA; 3) substantially effect the information already provided in the facility's top-screen submission; or 4) substantially effect the measures contained in the facility's SSP. *Id.* at 17702.
44. *Id.* at 17734. (§27.250).
45. *Id.* at 17712.
46. *Id.* at 17734-5. (§27.255).
47. *Id.* at 17735. (§27.300).
48. *Id.* at 17736. (§27.325).
49. *See, e.g.,* 5 U.S.C. § 552, which includes exemptions to the Freedom of Information Act (FOIA) for national security information and proprietary information.
50. *Id.* at 17737. (§27.400).
51. *Id.* at 17739. (§27.405).
52. *Id.* (§27.410).
53. *See* www.whitehouse.gov/news/releases/2007/03/20070323-1.html.

***Joe D. Whitley*** *was the first general counsel of the Department of Homeland Security, and is now an attorney and part of the global security and enforcement team in the Washington, D.C. office of Alston & Bird LLP.* ***George A. Koenig*** *is former counsel to the general counsel of the Department of Homeland Security, and is now an attorney and part of the global security and enforcement team in the Washington, D.C. office of Alston & Bird LLP.*