The Heritage Foundation
LEADERSHIP FOR AMERICA

BACKGROUNDER

No. 2718 | AUGUST 14, 2012

Chemical Security in the U.S.: CFATS Regulations Too Complex, Overly Burdensome

Jessica Zuckerman

Abstract
In 2007, the Chemical Facility Anti-Terrorism Standards (CFATS) program to regulate chemical facilities in the U.S. took effect. While a degree of government oversight of high-risk chemicals is warranted, the CFATS regulations are overly complicated, and overly burdensome on the private sector, with little added security. CFATS expires in October 2012, and the Department of Homeland Security is pushing for a seven-year reauthorization. Rather than continuing flawed and misguided regulations, DHS and Congress should collaborate with the private sector to develop commonsense, market-conscious—and safer—policy solutions for U.S. chemical security.

This paper, in its entirety, can be found at **http://report.heritage.org/bg2718**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies
The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

On October 4, 2012, the Chemical Facility Anti-Terrorism Standards (CFATS) program will expire. Created in 2007, CFATS prescribes a regulatory framework for facilities that produce, handle, or store high-risk chemicals in the U.S. While a degree of government oversight over chemical security is warranted, the federal CFATS regulations have proved exceedingly complicated and overly burdensome on the private sector. Such excessive regulation inhibits the chemical sector, an integral component of the U.S. economy, from doing business and stymies economic growth.

CFATS has faced extensive programmatic and administrative challenges, such as a failure to define inspection standards and approve final site-security plans, which have recently been brought to light. Yet despite these extensive issues with the program, Department of Homeland Security (DHS) Under Secretary for National Protection and Programs (NPPD) Rand Beers has pushed for a seven-year reauthorization. Rather than continuing flawed and misguided regulations, the DHS and Congress should work with the private sector to develop commonsense, market-conscious

Key Points

- On October 4, 2012, the Chemical Facility Anti-Terrorism Standards (CFATS) program will expire. Created in 2007, CFATS regulates facilities that produce, handle, or store high-risk chemicals in the U.S.
- While a degree of government oversight over chemical security is warranted, the federal CFATS regulations have proved exceedingly complicated and overly burdensome on the private sector. Such excessive regulation inhibits the chemical sector, an integral component of the U.S. economy, from doing business and stymies economic growth.
- CFATS has had extensive challenges, such as a failure to define inspection standards and approve final site-security plans. Despite these extensive issues with the program, the Department of Homeland Security is pushing for a seven-year reauthorization.
- Rather than continuing flawed and misguided regulations, the DHS and Congress should work with the private sector to develop commonsense, market-conscious policy solutions for U.S. chemical security.

policy solutions for U.S. chemical security.

The Birth of CFATS

Chemical safety has long been a concern in the United States. In 1984, a gas leak at a Union Carbide pesticide factory in Bhopal, India, led to the accidental release of highly toxic industrial chemicals. Considered one of the world's worst industrial catastrophes, the accident left thousands dead and even more injured.[1] In the United States, the scale of the disaster spurred legislative proposals aimed at reducing the risk of chemical accidents.[2] In 1990, for instance, Congress included an amendment to the Clean Air Act, commonly known as the "Bhopal Amendment" or "General Duty Clause," placing an obligation on chemical facilities that handle hazardous chemicals to prevent chemical disasters.[3]

Certainly, the threat of chemical terrorism, theft, and diversion was present at the time. One of the 1993 World Trade Center bombers worked as a chemical engineer and was alleged to have used his company's stationary to order chemicals for use in explosives for the attack. The bombers in the attack were also reported to have stolen cyanide from a chemical facility with plans to release it into the ventilation system at the World Trade Center.[4] The 1995 sarin gas attack on the Tokyo subway system by the Aum Shinrikyo cult also demonstrated the potentially devastating results that chemical agents could pose in the hands of terrorists. After 9/11, concerns about the risk posed by terrorist attacks on U.S. chemical facilities were greatly elevated.

In October 2001, just one month after the attacks, the U.S. Army surgeon general reported that a terrorist attack resulting in a chemical release had the potential to kill or injure some 2.4 million people.[5] Though the report was later rescinded, concerns such as these spurred many in Congress to call for increased regulation of the chemical sector.

Immediately after 9/11, then-Senator John Corzine (D–NJ) proposed legislation calling for the adoption of inherently safer technology (IST), which would have required the chemical industry to eliminate or substitute their stores of dangerous chemicals with others deemed less hazardous by Congress. Debate over this and other proposals would continue until Congress passed the Homeland Security Appropriations Act of 2007. Contained within this bill was a mandate for the Secretary of Homeland Security to establish risk-based performance standards within six months of the bill's enactment for facilities that produce, handle, or store high-risk chemicals. At the same time, the act also mandated the development of vulnerability assessments and the establishment and implementation of chemical facility security plans.

Coming into effect on June 8, 2007, the CFATS interim final rule outlined the ability of the Secretary of Homeland Security to determine which chemical facilities are subject to CFATS requirements according to the risk posed to each facility.[6] A few months later, the DHS also released a list of 322 "chemicals of interest" (COIs). Chemicals, including such common industrial substances as chlorine, propane, and anhydrous ammonia, as well as specialty chemicals, were placed on the list due to a perceived security threat from their release, theft or diversion, or sabotage.[7]

Overly Burdensome and Confusing Standards

Certainly, it would be disingenuous to downplay the fact that chemicals and chemicals facilities are potential terrorist targets. Indeed, of the 51 publicly known

1. Tony Long, "Dec. 3, 1984: Bhopal, 'Worst Industrial Accident in History,'" *Wired*, December 3, 2008, http://www.wired.com/science/discoveries/news/2008/12/dayintech_1203 (accessed July 31, 2012).
2. Linda-Jo Schierow, "Chemical Facility Security," Congressional Research Service *Report for Congress*, August 2, 2006, http://www.fas.org/sgp/crs/homesec/RL31530.pdf (accessed July 31, 2012).
3. U.S. Department of Justice, *U.S. v. Motiva Enterprises LLC et al. (D.DEL.)*, November, 2010, http://www.justice.gov/enrd/4463.htm (accessed July 19, 2012), and Philip Radford, "Protecting Our Communities from a Chemical Disaster," *The Huffington Post* Blog, May 1, 2012, http://www.huffingtonpost.com/philip-radford/protecting-our-communitie_b_1465680.html (accessed July 31, 2012).
4. Schierow, "Chemical Facility Security."
5. Eben Kaplan, "Targets for Terrorists: Chemical Facilities," Council on Foreign Relations *Backgrounder*, December 11, 2006, http://www.cfr.org/united-states/targets-terrorists-chemical-facilities/p12207 (accessed July 31, 2012).
6. Dana A. Shea, "Chemical Facility Security: Issues and Options for the 112th Congress," Congressional Research Service *Report for Congress*, January 13, 2012, http://www.fas.org/sgp/crs/homesec/R41642.pdf (accessed July 31, 2012).
7. U.S. Department of Homeland Security, "How 'Appendix A: Chemicals of Interest' Was Developed," November 20, 2007, http://www.dhs.gov/files/programs/gc_1185909570187.shtm (accessed July 31, 2012).

Islamist-inspired thwarted terrorist plots against the United States since 9/11, at least three have involved chemical facilities or the diversion of potentially dangerous chemicals. Yet, while ensuring the security of chemical facilities is important, security requirements and measures should not be taken at the expense of private business and innovation when increased flexibility might achieve as much security. Similarly, when considering how best to ensure the safety and security of chemical facilities and American citizens, it is important to remember that more requirements and more regulation do not necessarily equal greater security.

While a degree of government oversight over chemical security is needed, current standards are exceedingly burdensome and complicated, and overprescribe federal solutions with which the private sector must comply, threatening innovation and economic expansion.

Currently, CFATS requires that each facility undergo a complicated and often confusing four-step process, any aspect of which the facility can be required to repeat, should its chemical supplies change:

Step 1: Top-Screen. Any facility that possesses a chemical of interest in an amount greater than the designated screening threshold quantity is required to complete and submit a Top-Screen form—an online preliminary screening assessment on the presence and amount of COIs and other facility details.[8] Through Top-Screen, a component of the DHS's online Chemical Security Assessment Tool (CSAT), the DHS surveys and assesses each facility's use of COIs.

As of September 2011, 38,000 facilities had completed a Top-Screen assessment. From an evaluation of the initial information provided through Top-Screen, more than 7,000 facilities received a preliminary high-risk designation.[9] These facilities then received an initial risk ranking, with Tier 1 indicating the highest level of risk and Tier 4 the lowest.

Step 2: Security Vulnerability Assessment (SVA). Of the more than 7,000 chemical facilities initially designated as high risk, each was then required to submit a security vulnerability assessment (SVA).[10] While Top-Screen is meant to assess a facility's risk based on the potential consequences of the improper use of a COI, a security vulnerability assessment is intended to assess the likelihood that unintended consequences would be prevented based on the security measures already in place at the facility.[11] Within a SVA, facilities owners are required to provide greater detail on COIs, as well as information on access and inventory control and security equipment on hand. Facility owners are further required to provide an assessment of the possible risk and consequences of an attack on their facility, in addition to an evaluation of current emergency response and security procedures.[12] Gathering and compiling this information to complete the SVA is a complex process, and can take upwards of 250 hours according to DHS estimates.[13]

The information submitted in the SVAs could lead to one of three outcomes:

1. A facility could be removed from the list of high-risk facilities;
2. The preliminary tier ranking could be confirmed; or
3. The preliminary tier ranking could be changed.

From the submitted SVA information, the DHS ultimately determined that 4,569 of the more than 7,000 initial facilities should in fact be designated high-risk, and gave them a preliminary-tier or final-tier ranking. Table 1 shows CFATS rankings as of September 2011.

Step 3: Site-Security Plan (SSP). Following the completion of an SVA, CFATS-covered facilities must submit a site-security plan (SSP) detailing planned security measures, both physical and procedural, intended to address identified vulnerabilities. As part of the CFATS program, DHS developed a set of 18 risk-based performance standards (RBPSs). The RBPSs represent

8. U.S. Department of Homeland Security, "Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule," *Federal Register*, November 20, 2007, http://www.dhs.gov/xlibrary/assets/chemsec_appendixafinalrule.pdf (accessed August 3, 2012).
9. Shea, "Chemical Facility Security."
10. Ibid.
11. John C. Fannin III, "Understanding CFATS: What It Means to Your Business," ADT Business Solutions *White Paper*, December 1, 2009, http://www.adt.com/commercial-security/resource-library/white-papers/library/understanding-cfats (accessed August 3, 2012).
12. Fannin, "Understanding CFATS," and U.S. Department of Homeland Security, "CSAT Security Vulnerability Assessment: Questions," June 2008, http://www.dhs.gov/xlibrary/assets/chemsec_csat_sva_questions.pdf (accessed August 3, 2012).
13. Ibid.

TABLE 1

Facilities Regulated by DHS Under CFATS

Risk Tier	Facilities with Final Tier Decision	Facilities Awaiting Final Tier Decision	Total Facilities
1	99	3	102
2	502	37	539
3	1,155	135	1,290
4	2,195	443	2,638
Total	3,951	618	4,569

Source: Dana A. Shea, "Chemical Facility Security: Issues and Options for the 112th Congress," Congressional Research Service *Report for Congress*, January 13, 2012, http://www.fas.org/sgp/crs/homesec/R41642.pdf (accessed July 19, 2012).

B 2718 heritage.org

CFATS Risk-Based Performance Standards[14]

1. Restricted-Area Perimeter
2. Secure Site Assets
3. Screen and Control Access
4. Deter, Detect, and Delay
5. Shipping, Receipt, and Storage
6. Theft and Diversion
7. Sabotage
8. Cyber
9. Response
10. Monitoring
11. Training
12. Personnel Surety
13. Elevated Threats
14. Specific Threats, Vulnerabilities, or Risks
15. Report of Significant Security Incidents
16. Significant Security Incidents
17. Officials and Organizations
18. Records

different aspects of potential vulnerability in the site's security. In order to satisfy the requirements of CFATS, facilities must prove that they have adequately addressed the risks outlined by the RBPS in their site-security plan. The manner in which these requirements are met is left to the discretion of the individual facility. However, the higher the facility's risk tier, the more robust the measures contained in the SSP are expected to be. Tier 3 and Tier 4 facilities also have the option of submitting an alternative security program (ASP), provided they comply with the tier system and continue to meet performance-based requirements. An ASP is an alternative to an SSP that allows facilities to take advantage of existing security investments.

Upon competition, a facility's SSP or ASP is then sent to the Infrastructure Security Compliance Division (ISCD) within DHS's National Protection and Programs Directorate for review. DHS does not dictate which security measures should be put in place, but ascertains whether the security measures indicated in the SSP meet the risk-based performance standards.

Step 4: Authorization and Compliance. Following DHS approval of a facility's SSP, that facility is given a deadline by which it must successfully implement that plan. If the DHS finds the facility in violation of any component of the plan, the DHS may order the company to comply within a given time frame. Failure to comply with such an order can result in a penalty of up to $25,000 per violation.

In order for an SSP to be approved and a facility to be considered fully CFATS-compliant, the ISCD must conduct a pre-authorization visit and an authorization inspection. As of July 2012, only 63 facilities had received conditional authorization based on initial ISCD visits and none had been deemed fully compliant.[15]

In addition to these initial inspections, facilities are required to resubmit their Top-Screens on a regular basis. For facilities ranked in Tier 1 or Tier 2, these must be resubmitted every two years, while facilities in Tiers 3 and 4 must resubmit them

14. U.S. Department of Homeland Security, "Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards," May 2009, http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf (accessed August 1, 2012).
15. Suzanne Spaulding, Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security, "Department of Homeland Security—Chemical Facility Anti-Terrorism Standards (CFATS) Program," testimony before the Subcommittee on Homeland Security, Committee on Appropriations, U.S. House of Representatives, July 26, 2012, http://appropriations.house.gov/UploadedFiles/HHRG-112-AP15-SSpaulding-20120726.pdf (accessed August 1, 2012).

every three years. Moreover, any increase in the quantity of chemicals above the minimum threshold requires the facility to complete a Top-Screen.

Right in Principle, Wrong in Practice

In testimony before the House Committee on Homeland Security in 2011, DHS's Under Secretary for the National Protection and Programs Directorate Rand Beers outlined the four principles that guided the development of the CFATS regulatory structure:

> Securing high-risk chemical facilities is a comprehensive undertaking that involves a national effort, including all levels of government and the private sector.
>
> Risk-based tiering to guide resource allocations.
>
> Reasonable, clear, and calibrated performance standards will lead to enhanced security.
>
> Recognition of the progress many companies have already made in improving facility security leverages those advancements.[16]

While largely good on paper, in implementing the CFATS program, DHS has struggled with more than one of these principles.

Cross-Collaboration. The security of the high-risk chemical facilities is a collaborative endeavor. Facilities that possess chemicals capable of causing catastrophic disasters might benefit from a degree of federal oversight, while private-sector facilities themselves have a vested interest in providing security for their facilities. State and local governments also have a vested interest, as any disaster or catastrophe would occur directly in their jurisdiction. The three must work together to enhance U.S. chemical security. The CFATS program, however, places the primary burden for solving security problems on the federal government. The government must determine facilities' risk levels, set performance standards, and assess security plans and compliance.

Enhancing chemical security does not mean that the private sector should yield its responsibility to the federal government. The Department of Homeland Security and the private sector ought to collaborate to develop commonsense, market-conscious policy solutions.

Risk-Based Tiering. The Department of Homeland Security asserts that the CFATS system of tiering is based on risk, allowing the DHS to better focus resources on the high-risk chemical facilities.[17] However, since the basis for a facility's tier ranking is not openly shared by the DHS, even with individual chemical facility owners, the validity of this assertion must be tested. Details on how DHS analyzes the information provided by facilities in a security vulnerability assessment, how tiering decisions are made, and potential changes that would affect a facility's tier level are thus unavailable to facility owners to inform decisions about management practices.[18] In addition, first responders and community leaders have also expressed concern about the lack of transparency of facility tiering and risk assessments, citing the fact that the lack of information sharing may impede emergency response and community preparedness.[19]

Aggravating frustration with DHS's risk-based tier system, in June 2011 DHS announced that it had identified anomalies in one of its risk-assessment tools.[20] The discovery resulted in the department reducing the risk-tier levels of approximately 500 facilities. Overall the number of Tier 1 facilities was reduced by 50 percent, from 211 to 102. Some facilities were even removed from high-risk classification altogether and were no longer deemed to require CFATS compliance.[21] Unfortunately this comes as little surprise, given past assessments indicating that DHS's risk-analysis capabilities and

16. Rand Beers, "H.R. 908, a Bill to Extend the Authority of the Secretary of Homeland Security to Maintain the Chemical Facility Anti-Terrorism Standards (CFATS) Program," testimony before the Committee on Energy and Commerce, U.S. House of Representatives, March 30, 2011, http://www.dhs.gov/ynews/testimony/testimony_1301517368947.shtm (accessed August 1, 2012).
17. U.S. Department of Homeland Security, "Risk for Chemical Facility Anti-Terrorism Standards (CFATS)," February 18, 2009, http://www.dhs.gov/files/programs/gc_1185897486043.shtm#2 (accessed August 1, 2012).
18. American Chemistry Council, "A Survey of CFATS Progress in Securing the Chemical Sector," September 6, 2011, http://www.americanchemistry.com/Policy/Security/A-Survey-of-CFATS-Progress-in-Securing-the-Chemical-Sector.pdf (accessed August 1, 2012).
19. Shea, "Chemical Facility Security."
20. U.S. Department of Homeland Security, "DHS Notifies Chemical Facilities of Revised Tiering Assignments," July 5, 2011, http://www.dhs.gov/files/programs/cfats-revised-tiering-assignments.shtm (accessed August 1, 2012).
21. Shea, "Chemical Facility Security."

methods are largely inadequate for informing departmental decisions.[22]

Performance Standards. A key concept behind the CFATS program was that the DHS would not dictate specific security measures to individual chemical facilities. The DHS issued its 18 risk-based performance standards ostensibly based on this very concept:

> Performance standards are particularly appropriate in a security context because they provide individual facilities the flexibility to address their unique security challenges. Using performance standards rather than prescriptive standards also helps to increase the overall security of the sector by varying the security practices used by different chemical facilities. Security measures that differ from facility to facility mean that each presents a new and unique problem for an adversary to solve.[23]

Due to the risk-based nature of CFATS, facilities are expected to use a good deal of their own judgment in designing their SSPs and complying with the 18 standards. Indeed, the DHS indicates that no SSP may be approved or denied on the basis of the presence or absence of specific security measures.[24]

In theory, this practice is intended to promote the development and implementation of best practices, and also allow each facility to determine how to best meet security standards without inhibiting business and innovation. The reality, however, has been quite different.

Despite the DHS publishing its "Risk-Based Performance Standards Guidance" in May 2009, chemical facilities have largely been left uncertain over what is expected of them in meeting the DHS's standards. Approximately five years after CFATS was authorized, not a single SSP has been approved. Similarly, issues in training and hiring capable and experienced inspectors has resulted in confusing and conflicting feedback from ISCD inspectors in the course of pre-authorization visits and authorization inspections.

Leveraging Existing Advancements. Also contained within the CFATS regulations is the option for regulated facilities to submit an ASP in lieu of the standard SSP. This provision is intended to "leverage existing security investments," in order to make the most of private innovation in this field.[25] Some companies, such as Arch Chemicals, Dow Chemicals, and Eastman Chemicals have all invested sizeable amounts of money into the improvement of technology through high-tech cameras, new fences, better IDs, and more guards. Moreover, the American Chemistry Council, the Society of Chemical Manufacturers and Affiliates, and the Chlorine Institute established the Responsible Care Code, which created security guidelines for their members in areas from cybersecurity to communication to training and drills.[26] Such initiatives indicate that serious efforts are being made in the private sector to meet chemical facilities' significant security needs.

The ASP provision is an important means that allows chemical facilities to better determine which security measures best meet their needs and leverage existing investments. Unfortunately, there is little evidence that the DHS sees it as anything more than a feel-good measure. DHS spokeswoman Amy Kudwa recently described the department's attitude to the measure thus: "We also are willing to consider ASP submissions by facilities that may need to comply with CFATS for, for example, possession of a *single chemical of interest* that represents *one security issue*."[27] This very narrow understanding of an acceptable ASP program provides insight into the DHS's reluctance to accept these options.

This lack of motivation on the part of the DHS to seriously consider ASPs inhibits the ability of companies to continue to employ security measures in which they have already invested time and effort, thereby discouraging the innovation and creative thinking that have been critical to the security of the private sector in the past. As such, it limits the field of security options to those rigidly established by the federal government.

The Department of Homeland Security must work to better

22. National Academy of Science, *Review of the Department of Homeland Security's Approach to Risk Analysis* (Washington, DC: National Academies Press, 2010), http://www.nap.edu/catalog.php?record_id=12972 (accessed August 1, 2012).
23. U.S. Department of Homeland Security, "Risk for Chemical Facility Anti-Terrorism Standards (CFATS)."
24. U.S. Department of Homeland Security, "Risk-Based Performance Standards Guidance."
25. Joseph Straw, "The Skinny on CFATS," Security Management, http://www.securitymanagement.com/article/skinny-cfats-006559 (accessed August 1, 2012).
26. American Chemistry Council, "Responsible Care® Security Code of Management Practices," http://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Responsible-Care-Security-Code/PDF-Responsible-Care-Security-Code.pdf (accessed August 1, 2012).
27. Straw, "The Skinny on CFATS." Emphasis added.

leverage private-sector innovation. In addition to promoting the use of ASPs, the department should encourage companies to apply for certification under the Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. The SAFETY Act lowers the liability risks of creating products and services for combating terrorism by limiting third-party claims for losses resulting from an act of terrorism where the technology was deployed to help prevent or mitigate the danger of a terrorist attack. By providing certified companies with civil liability protection, expansion of the SAFETY Act would help encourage these companies to create technologies and applications that protect chemical facilities from acts of terrorism.

Other Critical Concerns

In December 2011, an internal memo from ISCD director Penny Anderson detailing the challenges besetting the CFATS program was leaked to the media.[28] Ensuing articles and congressional hearings brought to light many of the issues determined in the so-called Anderson memo to "pose a measurable risk to the [CFATS] program."[29]

According to the Anderson memo, the CFATS program has been beset by a number of serious problems. As of late 2011, the ISCD had yet to conduct a compliance inspection, and in fact, had not even developed the processes and procedures to do so. Likewise, the ISCD has not yet approved a final site-security plan.[30] While the ISCD has since announced that it plans to complete review of the site-security plans for all Tier 1 facilities by the end of FY 2012, and Tier 2 no later than FY 2013, the lack of a means of judging industry compliance with the regulations remains troubling.[31]

This failure is likely related to the ISCD's reported inability to adequately conduct hires, or to properly train those it does hire within the CFATS program. Moreover, the ISCD lacks basic guidelines for conducting hires, and has failed to outline the requirements for many key positions, including that of chemical inspectors. Consequently, it is hardly surprising that the ISCD is purportedly burdened by individuals who are not qualified for the positions they hold. This has even extended to the point of individuals who lack any noteworthy managerial experience holding leadership positions.[32]

Many of the challenges faced by the ISCD are even less straightforward. One of the critical problems this group has faced has been a weakness in morale among employees. As the workplace culture has largely been one that "does not value professionalism, respect and openness," many employees holding "non-conforming" opinions have been made to feel uncomfortable thinking outside the box.[33] Additionally, many employees have an inaccurate idea about the nature of their position, viewing it as an extension of earlier law enforcement careers. This has led to false expectations, such as being able to wear uniforms as symbols of authority or the right to carry a firearm. Additionally, the ISCD has purchased first responder equipment, such as hazmat suits and rappelling ropes, despite the fact that the division has no first responder responsibilities.[34] Such demands indicate the failure of the agency itself to define the role and business culture of its officials.

Ultimately, the challenges that the ISCD faces are fundamental. Despite developing a 94-point action plan to address the issues outlined in the Anderson memo, the fact that these problems are so severe five years after CFATS was created remains disconcerting and only adds to the burden imposed on industry by the misguided CFATS regulatory framework.[35]

Calls for Further Regulation

In spite of the critical issues that have ensued after the implementation of the CFATS program, there have been many calls for further regulation of the chemical sector. While generally misguided, many of

28. Mike Levin, "Beset by Strife at Chemical Security Office, DHS Internal Report Claims Anti-Terrorism Program Now in Jeopardy," FoxNews, December 21, 2011, http://www.foxnews.com/politics/2011/12/21/exclusive-beset-by-strife-at-dhs-office-future-anti-terrorism-program-now-in/ (accessed August 1, 2012).
29. Ibid.
30. Ibid.
31. Beers, "The Chemical Facilities Anti-Terrorism Standards Program."
32. Levine, "Beset by Strife at Chemical Security Office."
33. Ibid.
34. Ibid.
35. Spaulding, "Department of Homeland Security—Chemical Facility Anti-Terrorism Standards (CFATS) Program."

these measures have received a good deal of attention in Congress.

Regulation of Exempted Facilities. In addition to mandating that the Secretary of Homeland Security establish risk-based performance standards for high-risk facilities, Section 550 of the Homeland Security Appropriations Act of 2007 expressly exempts a number of facilities from CFATS regulation:

- Facilities regulated under the Maritime Transportation Safety Act of 2002;
- Public water systems;
- Wastewater treatment facilities;
- Facilities owned and operated by the Department of Defense or the Department of Energy; and
- Facilities regulated by the Nuclear Regulatory Commission.

In the years since the program's creation, however, multiple calls have been made for the extension of CFATS regulations to exempted facilities, particularly public water and wastewater treatment facilities. These facilities currently fall under the regulatory authority of the Environmental Protection Agency (EPA) and are already subject to risk management and emergency planning requirements under the Safe Drinking Water and Clean Water Acts.[36]

Yet despite this fact, NPPD Under Secretary Beers recently indicated that the directorate has been working closely with the EPA to assess the feasibility of folding water and wastewater treatment facilities into the CFATS program.[37] Beers previously categorized their exemption as a "critical gap in the U.S. chemical facility security regulatory framework."[38]

These statements, however, go directly against past Administration assertions that the "EPA should be the lead agency for chemical security for both drinking water and wastewater systems, with DHS supporting EPA's efforts."[39] Indeed, it makes sense that the EPA would be the lead agency for drinking water and wastewater systems, given the connection between water systems and public health. Public water and water treatment facilities differ from the majority of CFATS-regulated facilities, and any shutdown due to regulatory non-compliance would likely have large effects on public health and well-being.

Inherently Safer Technology (IST) Mandate. Since former Senator Corzine's original proposal in 2001, the concept of an IST mandate has been often debated by industry and Congress. Such a mandate would demand that companies consider alternative, purportedly safer chemicals to replace the potentially dangerous chemicals of interest. In that respect, such a mandate would allow the Department of Homeland Security to potentially require changes in chemical processes, inputs, or end products.[40]

Many industry leaders have opposed this mandate, claiming that it would be potentially harmful to both industry and security.[41] The forced implementation of supposedly lower-risk chemicals has the potential to increase business costs, placing an increased burden on manufacturers. This, despite the fact that companies that wish to avoid the potentially devastating consequences of either a chemical accident or a terrorist attack already have a natural incentive to use the safest chemicals possible. In fact, more than 2,000 chemical facilities are no longer deemed high-risk and are no longer subject to CFATS, due to voluntary risk-reduction measures.[42]

36. American Water Works Association, "Chemical Facility Security," 2009, http://www.awwa.org/files/GovtPublicAffairs/PDF/2009Security.pdf (accessed August 1, 2012).
37. Beers, "The Chemical Facilities Anti-Terrorism Standards Program."
38. Rand Beers, "Preventing Chemical Terrorism: Building A Foundation of Security at Our Nation's Chemical Facilities," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, February 11, 2011, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Beers_1.pdf (accessed August 1, 2012).
39. Peter S. Silva, testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate, March 3, 2010, http://www.epa.gov/ocir/hearings/testimony/111_2009_2010/2010_0303_pss.pdf (accessed August 1, 2012).
40. Joe Kamalick, "Key US House Leader to Oppose Safer Technology Mandate," ICIS, November 8, 2010, http://www.icis.com/Articles/2010/11/08/9408382/key-us-house-leader-to-oppose-safer-technology-mandate.html (accessed August 1, 2012).
41. Joe Kamalick, "US Chemical Leaders Blast New Senate Security Proposal," July 16, 2010, ICIS, http://www.icis.com/Articles/2010/07/16/9377291/us-chemical-leaders-blast-new-senate-security-proposal.html (accessed August 1, 2012).
42. American Chemistry Council, "Enhancing Chemical Security: A Decade of Progress," http://www.americanchemistry.com/Policy/Security/Chemical-Security-Fact-Sheet.pdf (accessed August 1, 2012).

Provisions such as the IST mandate are only likely to create unnecessary and damaging burdens on private industry. Moreover, leading industry experts claimed that it is not likely to improve the security of chemical facilities. Such experts assert that the use of increased quantities of chemicals and mixing of chemicals necessary to substitute certain COIs have the potential to be equally dangerous, perhaps more so, than the COIs themselves.[43]

In testimony before the House Committee on Homeland Security, William Allmond IV, vice president of government and public relations at the Society of Chemical Manufacturers and Affiliates, explained that

> IST is a process-related engineering concept, not a security one. It is premised on the belief that, if a particular chemical process hazard can be reduced, the overall risk associated with that process will also be reduced. In its simplicity, it is an elegant concept, but the reality is almost never that simple. A reduction in hazard will reduce overall risk if, and only if, (i) that hazard is not displaced to another time or location and (ii) it does not result in the creation of some new hazard.[44]

This misperception of IST provisions is only aggravated by the fact that there is no widely accepted scientific process by which to assess and quantify inherently safer technology.[45]

EPA Authority Under the Clean Air Act. Unsatisfied with the security measures of the CFATS program, some have called upon the EPA to impose greater regulation on the chemical security sector under the authority granted to it by the "General Duty Clause" of the Clean Air Act.

In a letter to current EPA administrator Lisa Jackson in April, Christine Todd Whitman, who held Jackson's position under the George W. Bush Administration, detailed how the EPA was prepared to unveil IST requirements under the authority of the Clean Air Act immediately after 9/11. Whitman urged her successor to pick up where she once left off.[46] A May 2012 letter to President Obama by 100 labor, environmental, and public health organizations further emphasized Whitman's argument criticizing the fact that CFATS prohibits the DHS from requiring specific security measures and asserting that "the only way communities are protected from chemical disasters is to fully enforce the 1990 Clean Air Act."[47]

But, not only would the Clean Air Act proposal undermine one of the few things CFATS gets right—the restriction on the federal government from proscribing specific security measures—it would also likely impose overlapping and confusing requirements and additional cost burdens on facilities already regulated by CFATS.

Developing Market-Oriented Chemical Security Solutions

Despite the reforms proposed by the National Protections and Programs Directorate, the House Appropriations Committee indicates that it will still be more than a year before the ISCD fully authorizes and completes a compliance inspection on any one of the more than 4,500 chemical facilities subject to regulation under CFATS, and nearly seven years before all authorization and inspections are completed at all facilities.[48] In response, the committee directed the Undersecretary for NPPD, along with the Commandant

43. Bob Weeks, "Inherently Safer Technology (IST) Not Always That," Voice for Liberty in Wichita, June 30, 2009, http://wichitaliberty.org/regulation/inherently-safer-technology-ist-not-always-that/ (accessed August 1, 2012), and M. Sam Mannan, "Preventing Chemical Terrorism: Building a Foundation of Security at Our Nation's Chemical Facilities," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technology, Committee on Homeland Security, U.S. House of Representatives, February 11, 2011, http://homeland.house.gov/hearing/subcommittee-hearing-%E2%80%9Cpreventing-chemical-terrorism-building-foundation-security-our-nation (accessed August 1, 2012).
44. William E. Allmond IV, "The Chemical Facility Anti-Terrorism Standards Program: Addressing Its Challenges & Finding a Way Forward," testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, U.S. House of Representatives, March 6, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Allmond.pdf (accessed August 1, 2012).
45. Mannan, "Preventing Chemical Terrorism."
46. Christine Todd Whitman, letter to EPA administrator Lisa Jackson, April 3, 2012, http://www.eenews.net/assets/2012/04/16/document_gw_02.pdf (accessed August 1, 2012).
47. AFL–CIO et. al., letter to President Barack Obama, May 16, 2012, https://s3.amazonaws.com/s3.documentcloud.org/documents/357316/coalition-letter-obama-chemical-disaster.pdf (accessed August 1, 2012).
48. Department of Homeland Security, Appropriations Bill, 2013, 112th Congress, 2nd Session, May 2012, http://appropriations.house.gov/uploadedfiles/homeland-fy13-fullcommitteereport.pdf (accessed August 1, 2012).

of the Coast Guard, to undertake a review of CFATS regulation. Under the Maritime Transportation Security Act (MTSA) of 2002, the Coast Guard is charged with regulating the security of the maritime transportation sector. While important differences exist in the security oversight of the two sections, the Coast Guard's implementation of MTSA regulations has been viewed as consistent and effective. The review will thus offer important lessons for chemical facility regulation.

Yet while the review represents an important step, more remains to be done. As Congress and the Department of Homeland Security consider the reauthorization of the CFATS program, they should:

- **Take a truly risk-based approach to chemical security.** Congress and the DHS should re-examine the CFATS program in order to promote chemical security policies that both keep the nation safe and respect America's free-market principles. The program currently places the primary burden for solving security problems on the federal government. This is the wrong approach. Instead, security policy should be focused on determining precisely what the risk and vulnerabilities are for a particular sector, and on leaving room for creative, cost-effective private-sector solutions. This is not to say that high-risk chemical facilities should not be subject to a degree of federal oversight. But excessive regulation that prevents the private sector from doing business and fails to take a true risk-based approach is the wrong way forward.

- **Reject calls for greater regulation.** While proposals such as mandatory IST may look good on paper, their premise is misleading. Removing a particular chemical from use does not necessarily mean that the overall risk of a chemical facility will be reduced. Chemical facilities already have a natural incentive to avoid the devastating consequences of either a chemical accident or a terrorist attack. The forced implementation of supposedly lower-risk chemicals only places an increased burden on facilities and threatens to increase business costs. Similarly, calls for the EPA to use the authority granted to it by the Clean Air Act to place separate regulations on the chemical sector, along with calls to remove the CFATS exemption granted to water and wastewater treatment facilities, would only impose overlapping and confusing requirements and additional cost burdens on the private sector.

- **Expand SAFETY Act protections to encourage greater innovation.** Creating technologies that protect chemical facilities from terrorism will help all Americans. But the private sector will not invest the time and money associated with this research and development without proper liability limits. The SAFETY Act provides this protection. It lowers the liability risks of creating products and services for combating terrorism by limiting third-party claims for losses resulting from an act of terrorism where the technology was deployed to help prevent or mitigate the danger of a terrorist attack. The DHS should continue to encourage companies to learn about the act's protections.

- **Promote public–private partnerships to enhance aging U.S. infrastructure.** The United States' overall critical infrastructure, including the chemical sector, is inadequate and aging. Greater investment is needed not only to ensure that U.S. critical infrastructure is protected but that it is capable of bouncing back quickly when disaster strikes. This approach does not mean that there is a need for heavily subsidized public funding to attain this goal; instead, policymakers should shift the risks and rewards to the private sector. Through public–private partnerships, the U.S. should promote private-sector-led projects that create quality infrastructure capable of meeting the needs of the 21st century amid 21st-century threats.

- **Foster greater transparency and cooperation.** Among the greatest criticisms of the CFATS program has been a lack of transparency and insufficient cooperation with the private sector. Presently, critical information regarding vulnerability assessments and tiering decisions is not shared with regulated chemical facilities, and is thus unavailable to facility owners to inform decision making as a part of risk-management practices. This lack of transparency also threatens to impede emergency response and community preparedness. The DHS must also expand cooperation and communication with the chemical sector to ensure that private-sector concerns are addressed.

Clearly, chemical facilities are potential targets of terrorism. However, the regulations imposed by the CFATS program are the wrong approach to chemical facility security and only represent an unnecessary burden on the chemical industry. While there is a role for the government in promoting the security of high-risk chemical facilities, reactive measures that hamstring chemical industry will benefit no one. Instead of perpetuating the misguided and burdensome CFATS regulatory framework, the DHS and Congress should collaborate to develop commonsense, market-conscious policy solutions for U.S. chemical security.

*—**Jessica Zuckerman** is a Research Associate in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. The author is grateful to intern Maura Cremin for her help in preparing this paper.*