The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3901 | APRIL 9, 2013

Chemical Security: Risk-Based Solutions Key to Fixing Flaws

Jessica Zuckerman and David Inserra

Last month, the House Committee on Energy and Commerce held a hearing on Chemical Facilities Anti-Terrorism Standards (CFATS), a program that is overseen by the Department of Homeland Security (DHS). In this hearing, DHS representatives claimed to have "turned a corner" on the CFATS program, putting slow and burdensome procedures behind them and moving forward with timely implementation.

Yet despite this pledge, the fact is that the CFATS program remains mired in serious problems, including incomplete risk assessments, slow implementation, and disjointed outreach to the private sector. Instead of perpetuating burdensome and complicated regulations, CFATS should be reformed to take a truly risk-based approach to chemical security.

Good on Paper, Bad in Reality. CFATS went into effect in June 2007 to address threats posed by a potential terrorist attack at a chemical facility. The program was designed to be risk-based and give facilities the flexibility to decide how to best meet security standards without inhibiting business and innovation.

To this end, the program established 18 risk-based performance standards that a chemical facility must satisfy using whatever methods it chooses, subject to review by DHS. However, while CFATS was designed well on paper, DHS has had trouble implementing what has become an overly burdensome and inefficient program.

The CFATS process begins with several risk and vulnerability assessments that result in DHS issuing a tier ranking to a facility depending on the type and amount of chemicals it houses and its current level of security and vulnerabilities, with Tier 4 indicating the lowest level of risk and Tier 1 the highest. Once the final tier ranking is issued, covered facilities must submit a site-security plan (SSP), which describes the security improvements that each facility plans to make.

For facilities in Tiers 3 and 4, an alternative security program (ASP) is allowed, which lets facilities take greater advantage of existing security investments. DHS then authorizes the plan, conducts an authorization inspection, and determines whether it will approve the SSP or ASP. If DHS approves the plan, the facilities must implement it within a certain deadline, after which DHS will conduct compliance inspections.

DHS has not implemented the program well, however. Initially, ASPs were allowed in very few cases, though industry thought these should have wider use than DHS allowed. Risk-assessment tools, tiering policies, and feedback mechanisms were often faulty or inconsistent. Inexperienced and unprofessional inspectors as well as other staffing problems made the entire implementation process more difficult. Perhaps most glaring, DHS has still not completed any compliance inspections.

This paper, in its entirety, can be found at
http://report.heritage.org/ib3901

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

Recent Changes Show Improvements, but Major Concerns Remain. Following the leak of an internal DHS memo in 2011 that highlighted a number of issues that posed "a measureable risk to the [CFATS] program," congressional and media criticism forced DHS to make significant changes in the program. While these changes have resulted in some improvements, serious difficulties still exist, according to recent Government Accountability Office (GAO) testimony before Congress.[1]

For example, DHS has revised its system for risk assessment, allowing for a more accurate tiering of facilities, but major problems remain. CFATS tiering is supposed to consider consequences, threats, and vulnerabilities, but in each of these areas, DHS has not correctly considered these variables when assessing risk.

Specifically, the GAO found that DHS does not consider economic consequences or security vulnerability assessments in its risk-tiering system. Additionally, DHS is inconsistent in how it considers threats. About 90 percent of facilities are in the CFATS program because of worries about theft or diversion of chemicals. However, DHS does not consider the likelihood of theft or diversion when conducting its risk assessments. Furthermore, for the remaining 10 percent of facilities, DHS uses outdated threat information. The risk-based tiering system is central to CFATS, but DHS's risk assessment is highly flawed in all three elements. These critical problems call into question the accuracy and efficacy of the entire system.

DHS was also heavily criticized in 2011 for failing to approve the vast majority of security plans and for having yet to conduct a compliance inspection. Since then, DHS officials have revised the process for reviewing plans and have called their new process a "quantum leap" forward. However, according to the GAO, DHS "did not capture data that would enable them to measure how, if at all, the revised process is more efficient (i.e., less time consuming) than the former process."

Though DHS was able to approve only 18 security plans between July 2012 and December 2012, it has very optimistically estimated that its new procedures will allow it to approve 30–40 plans per month, an increase of over 900 percent. The GAO estimates that even if DHS increases its approval speed tenfold, it will take another seven to nine years for it to approve all chemical facility security plans, which currently total around 3,120.

This estimate does not even consider CFATS's compliance inspections, which DHS has still not started, though it estimates that it will begin these inspections in September 2013.

CFATS has also struggled to implement its personnel surety program. As one of the 18 risk-based performance standards, the personnel surety program is supposed to ensure that each chemical facility is adequately screening its personnel for ties to terrorism. Though DHS is working to finish this program, members of the regulated community pointed out in their testimony before Congress that "DHS does not currently have a workable Personnel Surety Program in place, resulting in no security plans being completely authorized or approved."[2]

This deficiency leaves chemical facilities with incomplete security plans and further calls into question the speed with which DHS will be able approve these plans.

CFATS Should Be Reformed to Be Less Cumbersome. Since the CFATS program came under fire in 2011, DHS has revised and improved the program, but more remains to be done. Serious problems continue to hamper CFATS's effectiveness. In order to improve chemical security in the U.S., DHS and Congress should:

- **Reform risk assessments to capture all relevant information, including consequences, threats, and vulnerabilities.** DHS has a history of being poor at conducting risk assessments, and this systemic problem must be resolved. Not correcting this problem will mean that important

1. Stephen L. Caldwell, "Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach," testimony before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, U.S. House of Representatives, March 14, 2013, p. 11, http://www.gao.gov/products/GAO-13-412T (accessed April 9, 2013).
2. Timothy J. Scott, "The Chemical Facility Anti-Terrorism Standards (CFATS) Program: A Progress Update," testimony before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, U.S. House of Representatives, March 14, 2013, p. 3, http://docs.house.gov/meetings/IF/IF18/20130314/100468/HHRG-113-IF18-Wstate-ScottT-20130314.pdf (accessed April 9, 2013).

security decisions are made with inaccurate and incomplete information.

- **Return CFATS to a truly risk-based approach.** A risk-based approach would allow chemical facilities and DHS to prioritize their actions and resources to concentrate on threats that pose the most serious risks. Instead of regulations that are inflexible and impose large costs, a risk-based approach would also better respect market principles and allow businesses the flexibility to manage risks in the most cost-effective manner.

- **Incentivize the private sector to do more in critical infrastructure security.** Expanding participation in the SAFETY Act program, which lowers the liability risks of creating products for combating terrorism, is a prime example of how DHS can spur innovation in homeland security. Additionally, improving public–private partnerships on aging critical infrastructure would enhance cooperation and address the nation's infrastructure challenges.

Another Corner Should Be Turned on CFATS. While DHS claims that it has turned a corner on the CFATS program, it is still far from achieving its goals. Approval of security plans (though faster than before) remains painfully slow, risk assessments are still incomplete, and the industry feedback process remains disjointed. The current approach is flawed and must be fixed by making CFATS a truly risk-based and cost-effective program.

—***Jessica Zuckerman*** *is Policy Analyst for the Western Hemisphere and* ***David Inserra*** *is a Research Assistant 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.*