United States Government Accountability Office

Testimony
Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, August 1, 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Improve Its Risk Assessments and Outreach for Chemical Facilities

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice

August 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Improve Its Risk Assessments and Outreach for Chemical Facilities

GAO Highlights

Highlights of GAO-13-801T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Facilities that produce, store, or use hazardous chemicals could be of interest to terrorists intent on using toxic chemicals to inflict mass casualties in the United States. As required by statute, DHS issued regulations that establish standards for the security of high-risk chemical facilities. DHS established the CFATS program to assess the risk posed by these facilities and inspect them to ensure compliance with DHS standards. ISCD, which manages the program, places high risk facilities in risk-based tiers and is to conduct inspections after it approves facility security plans. This statement summarizes the results of GAO's April 2013 report on the extent to which DHS (1) assigned chemical facilities to tiers and assessed its approach for doing so, (2) revised its process to review facility security plans, and (3) communicated and worked with owners and operators to improve security. GAO reviewed DHS reports and plans on risk assessments, security plan reviews, and facility outreach and interviewed DHS officials. GAO also received input from 11 trade associations representing chemical facilities, about ISCD outreach. The results of this input are not generalizable but provide insights.

What GAO Recommends

In its April 2013 report, GAO recommended that DHS enhance its risk assessment approach to incorporate all elements of risk, conduct a peer review after doing so, and explore opportunities to gather systematic feedback on facility outreach. DHS concurred with the recommendations and has actions underway to address them.

View GAO-13-801T. For more information, contact Stephen L. Caldwell at (202) 512-9610 or CaldwellS@gao.gov.

What GAO Found

In April 2013, GAO reported that, since 2007, the Department of Homeland Security's (DHS) Infrastructure Security Compliance Division (ISCD) assigned about 3,500 high-risk chemical facilities to risk-based tiers under its Chemical Facility Anti-Terrorism Standards (CFATS) program, but it has not fully assessed its approach for doing so. The approach ISCD used to assess risk and make decisions to place facilities in final tiers does not consider all of the elements of consequence, threat, and vulnerability associated with a terrorist attack involving certain chemicals. For example, the risk assessment approach is based primarily on consequences arising from human casualties, but does not consider economic consequences, as called for by the *National Infrastructure Protection Plan* (NIPP) and the CFATS regulation, nor does it consider vulnerability, consistent with the NIPP. ISCD had taken some actions to examine how its risk assessment approach could be enhanced, including commissioning a panel of experts to assess the current approach and recommend improvements. In April 2013, GAO reported that ISCD needed to incorporate the results of these efforts to help ensure that the revised assessment approach includes all elements of risk. After ISCD has incorporated all elements of risk into its approach, an independent peer review would provide better assurance that ISCD can appropriately identify and tier chemical facilities, better inform CFATS planning and resource decisions, and provide the greatest return on investment consistent with the NIPP.

GAO also reported that DHS's ISCD has revised its process for reviewing facilities' site security plans—which are to be approved before ISCD performs compliance inspections. The past process was considered by ISCD to be difficult to implement and caused bottlenecks in approving plans. ISCD viewed its revised process to be an improvement because, among other things, teams of experts reviewed parts of the plans simultaneously rather than sequentially, as occurred in the past. ISCD intends to measure the time it takes to complete reviews, but will not be able to do so until the process matures. GAO estimated that it could take another 7 to 9 years before ISCD is able to complete reviews on the approximately 3,120 plans in its queue at the time of GAO's review. Thus, the CFATS regulatory regime, including compliance inspections, would likely be implemented in 8 to 10 years. ISCD officials said that they are exploring ways to expedite the process such as streamlining inspection requirements.

Furthermore, GAO reported that DHS's ISCD has also taken various actions to work with owners and operators, including increasing the number of visits to facilities to discuss enhancing security plans, but trade associations that responded to GAO's query had mixed views on the effectiveness of ISCD's outreach. ISCD solicits informal feedback from facility owners and operators on its efforts to communicate and work with them, but it does not have an approach for obtaining systematic feedback on its outreach activities. GAO found that ISCD's ongoing efforts to develop a strategic communication plan may provide opportunities to explore how ISCD can obtain systematic feedback on these activities. A systematic approach for gathering feedback and measuring the results of its outreach efforts could help ISCD focus greater attention on targeting potential problems and areas needing improvement.

Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee:

I am pleased to be here today to discuss the findings from our April 2013 report on the Department of Homeland Security's (DHS) efforts to address the various challenges in implementing and managing the Chemical Facility Anti-Terrorism Standards (CFATS) program.[1] Chemicals held at facilities that use or store hazardous chemicals could be used to cause harm to surrounding populations during terrorist attacks, and could be stolen and used as chemical weapons, such as improvised explosive devices, or as the ingredients for making chemical weapons. Earlier this year, ammonium nitrate—one of the chemicals covered by the CFATS program—detonated during a fire at a fertilizer storage and distribution facility in West, Texas. The preliminary findings of an investigation by the U.S. Chemical Safety Board (CSB) showed that the explosion killed at least 14 people and injured more than 200 others, severely damaged or destroyed nearly 200 homes, 3 nearby schools, a nursing home, and an apartment complex.[2] According to CSB, the fire at the facility detonated about 30 tons of ammonium nitrate. As of July 2013, the cause of the fire had not been determined. This event serves as a tragic reminder of the extent to which chemicals covered by the CFATS program can pose a risk to surrounding populations.

The DHS appropriations act for fiscal year 2007[3] required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities, among other things.[4] In 2007, DHS

[1] GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: April 5, 2013).

[2] Rafael Moure-Eraso, Chairperson, U.S. Chemical Safety Board, testimony before the Senate Committee on Environment and Public Works, 113th Congress 1st Sess., June 27, 2013. The CSB is an independent federal agency charged with investigating industrial chemical accidents. The CSB board members are appointed by the President and confirmed by the Senate. According to the CSB website, CSB does not issue fines or citations, but makes recommendations to plants, regulatory agencies, industry organizations, and labor groups.

[3] Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

[4] According to DHS, a high-risk chemical facility is one that, in the discretion of the Secretary of Homeland Security, presents a high risk of significant adverse consequences for human life or health, national security, or critical economic assets if subjected to a terrorist attack, compromise, infiltration, or exploitation. 6 C.F.R. § 27.105.

established the CFATS program to assess the risk posed by chemical facilities; place high-risk facilities in one of four risk-based tiers; require high-risk facilities to develop security plans; review these plans; and inspect the facilities to ensure compliance with regulatory requirements. DHS's National Protection and Programs Directorate (NPPD) is responsible for the CFATS program. Within NPPD, the Infrastructure Security Compliance Division (ISCD), a division of the Office of Infrastructure Protection (IP), manages the program.

In 2011, a leaked internal memorandum prompted some Members of Congress and chemical facility owners and operators to become concerned about ISCD's ability to implement and manage a regulatory regime under the CFATS program. This memorandum, prepared by the then ISCD Director, raised concerns about the management of the program. The memorandum cited an array of challenges that ISCD had experienced implementing the CFATS program, including an inability to hire staff with the needed skills, an overly complicated security plan review process, and a compliance inspection process that had yet to be developed.

My testimony today summarizes the results of our April 2013, work on ISCD's efforts to address key mission issues that could affect the success of the program. Specifically, my testimony will address the extent to which DHS (1) assigned chemical facilities to risk-based tiers and assessed its approach for doing so, (2) revised the process used to review security plans, and (3) communicated and worked with facilities to help improve security. To conduct our work, we reviewed ISCD documents and data on tiered facilities and the approach used to determine a facility's risk; assessed ISCD's process for reviewing security plans and data on the number of plans reviewed, authorized, and approved from program inception through December 2012; and reviewed information on ISCD outreach activities. We also obtained the views of officials representing 11 trade associations with members regulated by CFATS on DHS efforts to work with facility owners and operators.[5] The information we obtained

[5]The 11 trade associations were among 15 that we contacted during our review and represent those that provided responses to our query about ISCD outreach activities. We selected the 15 trade associations because they are listed in the National Infrastructure Protection Plan (NIPP) as those with which DHS works on a regular basis on chemical security matters. According to the NIPP, working with these trade associations presents a more manageable number of contact points through which DHS can coordinate activities with a large number of the asset owners and operators in the chemical sector.

from association officials is not generalizable to the universe of chemical facilities covered by CFATS; however, it provides insights into DHS efforts to perform outreach and seek feedback on the implementation of the CFATS rule. We conducted this performance audit from October 2012 through April 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. More detailed information on the scope and methodology of our published report can be found therein.

Background

Section 550 of the DHS Appropriations Act for fiscal year 2007[6] requires DHS to issue regulations establishing risk-based performance standards for the security of facilities that the Secretary determines to present high levels of security risk, among other things.[7] The CFATS rule was published in April 2007,[8] and appendix A to the rule, published in November 2007, listed 322 chemicals of interest and the screening threshold quantities for each.[9] ISCD has direct responsibility for implementing DHS's CFATS rule, including assessing potential risks and identifying high-risk chemical facilities, promoting effective security planning, and ensuring that high-risk facilities meet applicable standards through site security plans approved by DHS. From fiscal years 2007 through 2012, DHS dedicated about $442 million to the CFATS program.

[6]Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

[7]The CFATS rule establishes 18 risk-based performance standards that identify the areas for which a facility's security posture are to be examined, such as perimeter security, access control, and cyber security. To meet these standards, facilities are free to choose whatever security programs or processes they deem appropriate so long as DHS determines that the facilities achieve the requisite level of performance in each applicable standard.

[8]72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified at 6 C.F.R. pt. 27).

[9]72 Fed. Reg. 65,396 (Nov. 20, 2007). According to DHS, CFATS not only covers facilities that manufacture chemicals but also covers facilities that store or use certain chemicals as part of their daily operations. This can include food-manufacturing facilities that use chemicals of interest in the manufacturing process, universities that use chemicals to do experiments, or warehouses that store ammonium nitrate, among others.

Appendix I describe the process for administering the CFATS program, as outlined in the rule.

ISCD uses a risk assessment approach to develop risk scores to assign chemical facilities to one of four final tiers. Facilities placed in one of these tiers (tier 1, 2, 3, or 4) are considered to be high risk, with tier 1 facilities considered to be the highest risk. According to an ISCD document that describes how ISCD develops its CFATS risk score, the risk score is intended to be derived from estimates of consequence (the adverse effects of a successful attack), threat (the likelihood of an attack), and vulnerability (the likelihood of a successful attack, given an attempt). ISCD's risk assessment approach is composed of three models, each based on a particular security issue: (1) release, (2) theft or diversion, and (3) sabotage, depending on the type of risk associated with the 322 chemicals.[10] Once ISCD estimates a risk score based on these models, it assigns the facility to a final tier.

ISCD Has Assigned Thousands of Facilities to Tiers, but ISCD's Approach to Risk Assessment Did Not Reflect All Elements of Risk

[10]For release, the model assumes that a terrorist will release the chemical of interest at the facility and then estimates the risk to the surrounding population. For theft or diversion, the model assumes that a terrorist will steal or have the chemical of interest diverted to him or herself and then estimates the risk of a terrorist attack using the chemical of interest in a way that causes the most harm at an unspecified off-site location. For sabotage, the model assumes that a terrorist will remove the chemical of interest from the facility and mix it with water, creating a toxic release at an unspecified off-site location, and then estimates the risk to a medium-sized U.S. city.

ISCD Has Tiered Thousands of High-Risk Facilities

In July 2007, ISCD began reviewing information submitted by the owners and operators of approximately 40,000 facilities. By January 2013, ISCD had designated about 4,400 of the 40,000 facilities as high risk and thereby covered by the CFATS rule.[11] ISCD had assigned about 3,500 of those facilities to a final tier, of which about 90 percent were tiered because of the risk of theft or diversion. The remaining 10 percent were tiered because of the risk of release or the risk of sabotage.[12]

ISCD's Risk Assessment Approach Did Not Consider All Elements of Risk

In April, 2013, we reported that the tiering approach ISCD uses to assess risk and assign facilities to final tiers did not consider all of the elements of risk associated with a terrorist attack involving certain chemicals. According to the National Infrastructure Protection Plan (NIPP), which, among other things, establishes the framework for managing risk among the nation's critical infrastructure, risk is a function of three components—consequence, threat, and vulnerability—and a risk assessment approach must assess each component for every defined risk scenario. Furthermore, the CFATS rule calls for ISCD to review consequence, threat, and vulnerability information in determining a facility's final tier. However, ISCD's risk assessment approach did not fully consider all of the core criteria or components of a risk assessment, as specified by the NIPP, nor did it comport with parts of the CFATS rule.

- *Consequence*. The NIPP states that at a minimum, consequences should focus on the two most fundamental components—human consequences and the most relevant direct economic consequences. The CFATS rule states that chemical facilities covered by the rule are those that present a high risk of significant adverse consequences for human life or health, or critical economic assets, among other things, if subjected to terrorist attack, compromise, infiltration, or exploitation.[13] Our report showed that ISCD's risk assessment approach was limited to focusing on one component of

[11]According to ISCD officials, approximately 35,600 facilities were not considered high risk because after preliminary evaluation, DHS concluded that they were considered not to be high enough risk to be covered by the program; thus they were no longer covered by the rule.

[12]According to ISCD officials, depending on the chemicals on-site, a facility can be final-tiered for more than one security issue.

[13]6 C.F.R. §§ 27.105, .205.

consequences—human casualties associated with a terrorist attack involving a chemical of interest—and did not consider consequences associated with economic criticality. ISCD officials said that the economic consequences part of their risk-tiering approach will require additional work before it is ready to be introduced. In September 2012, ISCD officials said they engaged Sandia National Laboratories to examine how ISCD could gather needed information and determine the risk associated with economic impact, but this effort is in its early stages.

- *Threat*. ISCD's risk assessment approach was not consistent with the NIPP because it did not consider threat for the majority of regulated facilities. According to the NIPP, risk assessments should estimate threat as the likelihood that the adversary would attempt a given attack method against the target. The CFATS rule requires that, as part of assessing site vulnerability, facilities conduct a threat assessment, which is to include a description of the internal, external, and internally assisted threats facing the facility and that ISCD review the site vulnerability assessment as part of the final determination of a facility's tier.[14] Our report showed that (1) ISCD was inconsistent in how it assessed threat using the different models because while it considers threat for the 10 percent of facilities tiered because of the risk of release or sabotage, it did not consider threat for the approximately 90 percent of facilities tiered because of the risk of theft or diversion, and (2) ISCD did not use current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage. ISCD officials said that they were considering reexamining their approach and exploring how they could use more current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage.

- *Vulnerability*. ISCD's approach was also not consistent with the NIPP because it did not consider vulnerability when developing risk scores. According to the NIPP, risk assessments should identify vulnerabilities, describe all protective measures, and estimate the likelihood of an adversary's success for each attack scenario. Similar to the NIPP, the CFATS rule calls for ISCD to review facilities' security vulnerability assessments as part of its tiering process.[15] This

[14]6 C.F.R. §§ 27.215, .220.

[15]6 C.F.R. § 27.220.

assessment is to include the identification of potential security vulnerabilities and the identification of existing countermeasures and their level of effectiveness in both reducing identified vulnerabilities and meeting the aforementioned risk-based performance standards. We reported that the security vulnerability assessment contains numerous questions aimed at assessing vulnerability and security measures in place but the information was not used to assign facilities to risk-based tiers. ISCD officials said they do not use the information because it is "self-reported" by facilities and they have observed that it tends to overstate or understate vulnerability. Thus, ISCD's risk assessment approach treats every facility as equally vulnerable to a terrorist attack regardless of location and on-site security. ISCD officials told us that they consider facility vulnerability during the latter stages of the CFATS regulatory process, particularly with regard to the development and approval of the facility site security plan.

ISCD Had Begun to Take Actions to Examine How Its Approach Can Be Enhanced

In April 2013, we reported that ISCD had begun to take some actions to examine how its risk assessment approach can be enhanced. For example, ISCD had commissioned a panel of subject matter experts to examine the strengths and weaknesses of its risk assessment approach. We stated that ISCD appeared to be moving in the right direction, but would need to incorporate the various results of these efforts to help it ensure that the revised risk assessment approach includes all of the elements of risk. We further stated that once ISCD develops a more complete approach for assessing risk, it would then be better positioned to commission an independent peer review. In other past work, we have found that peer reviews are a best practice in risk management[16] and that independent expert review panels can provide objective reviews of complex issues.[17] As we previously stated in these reports, independent peer reviews cannot ensure the success of a risk assessment approach, but they can increase the probability of success by improving the technical quality of projects and the credibility of the decision-making

[16]See GAO, *Coast Guard*: *Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: Nov. 17, 2011). Peer reviews can identify areas for improvement and can facilitate sharing best practices.

[17]See GAO, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2011).

process.[18] In our April 2013 report, we recommended that DHS enhance its risk assessment approach to incorporate all elements of risk, and conduct a peer review after doing so. DHS concurred with our recommendations and stated that it had efforts under way to address them.

ISCD Had Revised Its Security Plan Review Process, but Plan Approvals Could Take Years

ISCD Revised Its Security Plan Review Process because of ISCD Managers' Concerns, and Plans to Measure Related Improvements Moving Forward

In April 2013 we reported that ISCD had made various revisions to its security plan review process to address concerns expressed by ISCD managers about slow review times. Under the CFATS rule, once a facility is assigned a final tier, it is to submit a site security plan to describe security measures to be taken and how it plans to address applicable risk-based performance standards.[19] In November 2011, ISCD acknowledged that the security plan review process it was using was overly complicated and created bottlenecks and officials stated that revising the process was a top program priority.[20] Shortly thereafter, ISCD developed an interim review process. ISCD officials subsequently told us

[18]See GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, GAO-12-14 (Washington, D.C.: November 17, 2011) and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C.: Mar. 31, 2004).

[19]6 C.F.R. § 27.210(a)(3), .225.

[20]The specific security measures and practices discussed in DHS's guidelines state that they are neither mandatory nor necessarily the "preferred solution" for complying with the risk-based performance standards. Rather, according to DHS, they are examples of measures and practices that a facility may choose to consider as part of its overall strategy to address the standards. High-risk facility owners and operators have the ability to choose and implement other measures to meet the risk-based performance standards based on circumstances, security issues and risks, and other factors, so long as DHS determines that the suite of measures implemented achieves the levels of performance established by the standards.

that the interim process was unsustainable, labor-intensive, and time-consuming because individual reviewers were sequentially looking at pieces of thousands of plans that funneled to one quality reviewer.[21] In July 2012, ISCD began using a newly revised process, which entailed using contractors, teams of ISCD employees (e.g., physical, cyber, and chemical specialists), and ISCD field inspectors to review plans simultaneously.[22]

ISCD officials said that they believed the revised process was a "quantum leap" forward, but they 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 processes. Moving forward, ISCD officials said they intended to measure the time it takes to complete parts of the revised site security plan review process and had recently implemented a plan to measure various aspects of the process. We reported that collecting data to measure performance about various aspects of this process is a step in the right direction, but it may take time before the process has matured to the point where ISCD is able to establish baselines and assess progress.

Security Plan Reviews Could Take Years to Complete, but ISCD Is Examining How It Can Accelerate the Review Process

We also reported in April 2013 that even with the most recent revisions to the review process, it could take years to review the plans of thousands of facilities that had already been assigned a final tier. ISCD hoped to address this by examining how it could further accelerate the review process. According to ISCD officials, between July 2012 and December 2012, ISCD had approved 18 security plans, with conditions.[23] ISCD officials told us that they anticipate that the revised security plan review

[21]Using the interim review process, ISCD officials estimated that they authorized about 60 security plans and notified the facilities that inspectors would schedule visits to determine if the security measures described in the plan were in place.

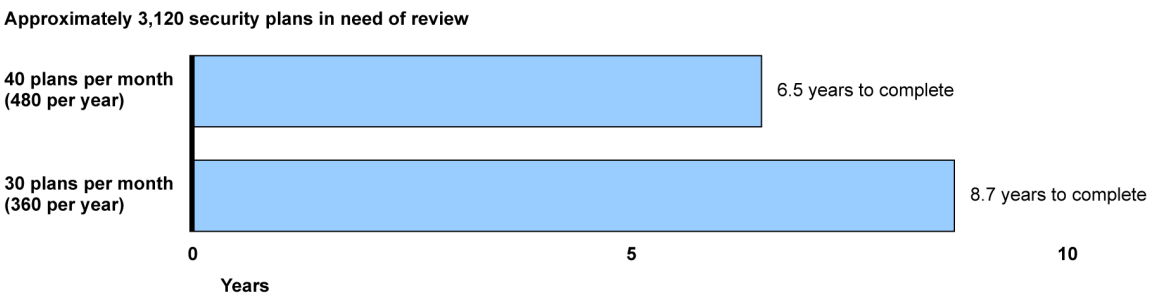
[22]According to ISCD officials, this newly revised process, like its predecessor, entailed a "holistic" review whereby individual reviewers were to consider how layers of security measures met the intent of each of the CFATS performance standards.

[23]All authorization letters include a condition noting that ISCD has not fully approved the personnel surety risk-based performance standard of plans because ISCD has not yet determined what the facilities are to do to meet all aspects of personnel surety. The personal surety risk-based performance standard requires that regulated chemical facilities implement measures designed to identify people with terrorist ties, among other things.

process could enable ISCD to approve security plans at a rate of about 30 to 40 a month.

Using ISCD's estimated approval rate of 30 to 40 plans a month, our April 2013 report showed that it could take anywhere from 7 to 9 years to complete reviews and approvals for the approximately 3,120 plans[24] submitted by facilities that had been final-tiered that ISCD had not yet begun to review.[25] Figure 1 shows our April 2013 estimate of the number of years it could take to approve all of the security plans for the approximately 3,120 facilities that, as of January 2013, had been final-tiered, assuming an approval rate of 30 to 40 plans a month.

Figure 1: Estimate of Number of Years to Approve Security Plans



Source: GAO.

It is important to note that our 7- to 9-year estimate did not include other activities central to the CFATS mission, either related to or aside from the security plan review process. In addition, our estimate did not include developing and implementing the compliance inspection process, which occurs after security plans are approved and is intended to ensure that facilities covered by the CFATS rule are compliant with the rule, within the context of the 18 performance standards. ISCD officials estimated that the first compliance inspections would commence in 2013, which means

[24]ISCD data showed that 380 security plans had started the review process and were at different phases of review.

[25]ISCD officials stated that the approval rate could reach 50 plans a month in the third quarter of fiscal year 2013, as the review process becomes more efficient. We did not calculate the time to complete reviews of the approximately 3,120 plans that had been final-tiered using ISCD's estimate of 50 per month because of uncertainty over when and if ISCD would reach this goal during the third quarter of fiscal year 2013.

that the CFATS regulatory regime would likely be fully implemented for currently tiered facilities (to include compliance inspections) in 8 to 10 years. ISCD officials stated that they were actively exploring ways to expedite the speed with which the backlog of security plans could be cleared, such as reprioritizing resources and streamlining inspection and review requirements.

ISCD Has increased Its Efforts to Communicate and Work with Facilities and May Have an Opportunity to Systematically Gather Feedback on Its Outreach Efforts

ISCD's External Communication Efforts with Facilities Have Increased since 2007, but Selected Trade Associations Had Mixed Views about ISCD Efforts

Our April 2013 report stated that ISCD's efforts to communicate and work with owners and operators to help them enhance security had increased since the CFATS program's inception in 2007. ISCD had taken various actions to communicate with facility owners and operators and various stakeholders—including officials representing state and local governments, private industry, and trade associations—to increase awareness about CFATS. For example, among other things, ISCD has increased the number of visits to facilities to discuss enhancing security plans.[26] However, trade associations' responses to questions we sent them about the program showed mixed views about ISCD's efforts to communicate with owners and operators through ISCD's outreach efforts. For example, 3 of the 11 trade associations that responded to our questions indicated that ISCD's outreach program was effective in

[26]Among other outreach activities, ISCD manages the Chemical Security website, which includes a searchable database to answer questions about the CFATS program. ISCD also manages a Help Desk (call service center), which is operated on a contract basis by the Oak Ridge National Laboratory.

general, 3 reported that the effectiveness of ISCD's outreach was mixed, 4 reported that ISCD's outreach was not effective, and 1 respondent reported that he did not know.[27]

ISCD Sought Informal Feedback, but Did Not Solicit Systematic Feedback on the Effectiveness of Its Outreach Efforts

Our report showed that ISCD sought informal feedback on its outreach efforts but did not systematically solicit feedback to assess the effectiveness of outreach activities,[28] and it did not have a mechanism to measure the effectiveness of these activities. Trade association officials reported that in general ISCD seeks informal feedback on its outreach efforts and that members provide feedback to ISCD. According to ISCD officials, feedback had been solicited from the regulated community generally on an informal basis, but inspectors and other staff involved in ISCD's outreach activities were not required to solicit feedback during meetings, presentations, and assistance visits on the effectiveness of the outreach. ISCD, as part of its annual operating plan, has established a priority for fiscal year 2013 to develop a strategic communications plan intended to address external communication needs including industry outreach, which may provide an opportunity to explore how ISCD can obtain systematic feedback on these activities. We concluded that a systematic approach for gathering feedback and measuring the results of its outreach efforts could help ISCD focus greater attention on targeting potential problems and areas needing improvement. We recommended that DHS explore opportunities to gather systematic feedback on facility outreach. DHS agreed and stated that it agreed with our recommendation and identified actions under way to address it.

Chairman Meehan, Ranking Member Clarke, and members of the subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

[27]We originally sent questions to 15 trade associations representing various members of the chemical industry and received responses from 11 of the 15. The trade associations that responded provided responses that represent, to their knowledge, the general view of their members. In some instances, the associations provided responses directly from member companies.

[28]ISCD solicits voluntary feedback via a survey provided to Help Desk users on their experience with call center representatives. The survey asks: Did the service meet expectations, were questions answered in a timely manner, and was the call service representative friendly and knowledgeable?

Contacts and Staff Acknowledgments

For information about this statement please contact Stephen L. Caldwell, at (202) 512-9610 or CaldwellS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions included John F. Mortin, Assistant Director; Chuck Bausell; Jose Cardenas; Michele Fejfar; Jeff Jensen; Tracey King; Marvin McGill; Jessica Orr; and Ellen Wolfe.

Appendix I: Department of Homeland Security's (DHS) Process for Administering the Chemical Facility Anti-Terrorism Standards (CFATS) Program

This appendix discusses DHS's process for administering the CFATS program. DHS's CFATS rule outlines a specific process for administering the program. Any chemical facility that possesses any of the 322 chemicals in the quantities that meet or exceed the threshold quantity outlined in Appendix A of the rule is required to use DHS's Chemical Security Assessment Tool (CSAT)—a web-based application through which owners and operators of chemical facilities provide information about the facility.[1] Once a facility is registered in CSAT, owners and operators are to complete the CSAT Top Screen—which is the initial screening tool or document whereby the facility is to provide DHS various data, including the name and location of the facility and the chemicals and their quantities at the site.[2] DHS is to analyze this information using its risk assessment approach, which is discussed in more detail below, to initially determine whether the facility is high risk.[3] If so, DHS is to notify the facility of its preliminary placement in one of four risk-based tiers—tier 1, 2, 3, or 4.[4] Facilities preliminarily placed in any one of these tiers are considered to be high risk, with tier 1 facilities considered to be the highest risk. Facilities that DHS initially determines to be high risk are required to then complete the CSAT security vulnerability assessment, which includes the identification of potential critical assets at the facility and a related vulnerability analysis.[5] DHS is to review the security vulnerability assessment and notify the facility of DHS's final determination as to whether or not the facility is considered high risk, and if the facility is determined to be a high-risk facility, about its final placement in one of the four tiers.[6]

[1]6 C.F.R. § 27.200(b).

[2]For example, under the CFATS rule, a facility that possesses butane at a quantity equal to or exceeding 10,000 pounds must submit information to DHS because the substance is considered flammable if subject to release. A facility possessing another chemical, oxygen difluoride, would have to submit information to DHS if it possessed a quantity equal to or exceeding 15 pounds of the substance, which, according to the rule, is considered vulnerable to theft for use as a weapon of mass effect.

[3]6 C.F.R. § 27.205(a).

[4]6 C.F.R. § 27.220(a), (c).

[5]6 C.F.R. § 27.215. Preliminary tier 4 facilities also have the option of submitting an alternate security program in lieu of a security vulnerability assessment. 6 C.F.R. § 27.235(a)(1).

[6]6 C.F.R. § 27.220(b), (c).

Once assigned a final tier, the facility is required to use CSAT to submit a site security plan or participate in an alternative security program in lieu of a site security plan.[7] The security plan is to describe the security measures to be taken to address the vulnerabilities identified in the vulnerability assessment, and identify and describe how security measures selected by the facility are to address the applicable risk-based performance standards.[8] DHS then is to conduct a preliminary review of the security plan to determine whether it meets the regulatory requirements. If these requirements appear to be satisfied, DHS is to issue a letter of authorization for the facility's plan. DHS then is to conduct an authorization inspection of the facility and subsequently determine whether to approve the security plan. If DHS determines that the plan does not satisfy CFATS requirements, DHS then notifies the facility of any deficiencies and the facility must submit a revised plan correcting them.[9] If the facility fails to correct the deficiencies, DHS may disapprove the plan.[10] Following approval, DHS may conduct further inspections to determine if the facility is in compliance with its approved security plan.[11] As of April 2013, DHS had not conducted any compliance inspections. Figure 2 illustrates the CFATS regulatory process.

[7]An Alternative Security Program (ASP) is a third-party, facility, or industry organization's security program that has been determined to meet the requirements of, and provides for an equivalent level of security to that established by the CFATS regulation. CFATS allows regulated chemical facilities to submit an ASP in lieu of a Site Security Plan. 6 C.F.R. § 27.235

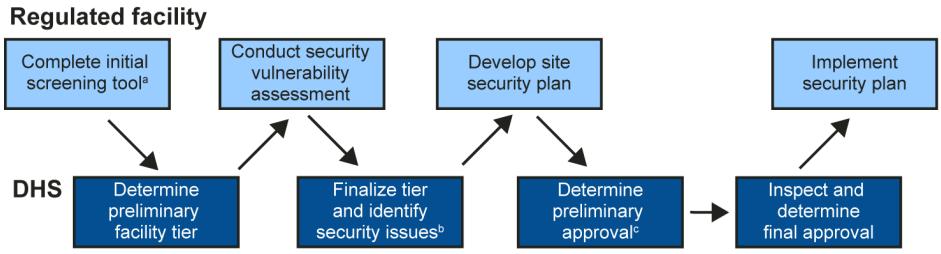
[8]6 C.F.R. § 27.225.

[9]According to Infrastructure Security Compliance Division (ISCD) officials, site security plans can also be sent back to facilities to be revised for any number of reasons. For example, during the preliminary review, if ISCD finds that a plan does not contain all the requisite data needed to meet regulatory requirements, ISCD can return the plan to the facility for more information.

[10]6 C.F.R. § 27.245.

[11]6 C.F.R. § 27.250.

Figure 2: Department of Homeland Security's (DHS) Chemical Facility Anti-Terrorism Standards (CFATS) Process



Source: GAO analysis of DHS CFATS regulatory process.

[a]Facilities are to submit an initial screening tool that provides basic information about the facilities and the chemicals they possess.

[b]This step includes determining if a facility is high risk, and if so, DHS assigns a tier and identifies security issues

[c]At this stage, if requirements are satisfied, DHS issues a letter of authorization for the facility's plan.

Related GAO Products

Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened. GAO-13-353, Washington, D.C.: April 5, 2013.

Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure. GAO-13-11. Washington, D.C.: October 25, 2012.

Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results. GAO-12-567T. Washington, D.C.: September 11, 2012.

Critical Infrastructure: DHS Needs to Refocus Its Efforts to Lead the Government Facilities Sector. GAO-12-852. Washington, D.C.: August 13, 2012.

Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results. GAO-12-515T. Washington, D.C.: July 26, 2012.

Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments. GAO-12-378. Washington, D.C.: May 31, 2012.

Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities. GAO-11-537R. Washington, D.C.: May 19, 2011.

Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened. GAO-10-772. Washington, D.C.: September 23, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report. GAO-09-654R. Washington, D.C.: June 26, 2009.

Information Technology: Federal Laws, Regulations, and Mandatory Standards to Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors. GAO-08-1075R. Washington, D.C.: September 16, 2008.

Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-904T. Washington, D.C.: June 25, 2008.

Critical Infrastructure: Sector Plans Complete and Sector Councils Evolving. GAO-07-1075T. Washington, D.C.: July 12, 2007.

Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. GAO-07-706R. Washington, D.C.: July 10, 2007.

Critical Infrastructure: Challenges Remain in Protecting Key Sectors. GAO-07-626T. Washington, D.C.: March 20, 2007.

Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks. GAO-07-375. Washington, D.C.: January 24, 2007.

Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. Washington, D.C.: October 16, 2006.

Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information. GAO-06-383. Washington, D.C.: April 17, 2006.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.