United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, March 14, 2013

CRITICAL INFRASTRUCTURE PROTECTION

Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach

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

March 2013

CRITICAL INFRASTRUCTURE PROTECTION

Preliminary Observations on DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-412T, a testimony before the Subcommittee on Environment and the Economy, Committee on Energy and Commerce, 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 in 2007 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. A November 2011 ISCD internal memorandum raised concerns about ISCD's ability to fulfill its mission.

This statement is based on GAO's ongoing work conducted for several congressional committees and subcommittees and provides preliminary observations regarding the extent to which DHS has (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. To conduct this ongoing work, GAO reviewed DHS reports and plans on risk assessments, security plan reviews, and facility outreach and interviewed DHS officials. GAO received input from 11 trade associations representing chemical facilities about ISCD outreach. The results of this input are not generalizable but provide insights about DHS outreach efforts.

View GAO-13-412T. For more information, contact Stephen L. Caldwell, (202)-512-9610, CaldwellS@gao.gov

What GAO Found

Since 2007, the Department of Homeland Security's (DHS) Infrastructure Security Compliance Division (ISCD) has assigned about 3,500 high-risk chemical facilities to risk-based tiers under its Chemical Facilities 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 include vulnerability, consistent with the NIPP. ISCD has begun to take some actions to examine how its risk assessment approach can be enhanced. Specifically, ISCD has, among other things, engaged Sandia National Laboratories to examine how economic consequences can be incorporated into ISCD's risk assessment approach and commissioned a panel of experts to assess the current approach, identify strengths and weaknesses, and recommend improvements. Given the critical nature of ISCD's risk assessment approach in laying the foundation for further regulatory steps in improving facility security, it is important that its approach for assigning facilities to tiers is complete within the NIPP risk management framework and the CFATS regulation.

DHS's ISCD has revised its process for reviewing facilities' site security plans—which are to be approved by ISCD before it performs compliance inspections—but it did not track data on the prior process so is unable to measure any improvements. The past process was considered by ISCD to be difficult to implement and caused bottlenecks in approving plans. ISCD views its revised process to be a significant improvement because, among other things, teams of experts review parts of the plans simultaneously rather than sequentially, as occurred in the past. Moving forward, ISCD intends to measure the time it takes to complete reviews, but will not be able to do so until the process matures. Using ISCD's expected plan approval rate of 30 to 40 plans a month, 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. ISCD officials said that they are exploring ways to expedite the process, such as reprioritizing resources.

DHS's ISCD has also taken various actions to work with facility 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. Prior GAO work on customer service efforts in the government indicates that systematic feedback from those receiving services can provide helpful information as to the kind and quality of services they want and their level of satisfaction with existing services. GAO will continue to assess ISCD's efforts in these areas and consider any recommendations needed to address these issues. GAO expects to issue a report on its results in April 2013.

Chairman Shimkus, Ranking Member Tonko, and Members of the Subcommittee:

I am pleased to be here today to discuss our preliminary observations 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. The events of September 11, 2001, triggered a national reexamination of the security of facilities that use or store hazardous chemicals in quantities that, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death. Chemicals held at these facilities can be used to cause harm to surrounding populations during terrorist attacks, can be stolen and used as chemical weapons or as precursors (the ingredients for making chemical weapons), or stolen and used to build an improvised explosive device. To mitigate this risk, the DHS appropriations act for fiscal year 2007[1] required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities, among other things.[2] In 2007, DHS established the CFATS program to assess the risk, if any, 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 the 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. In July 2012, we reported that ISCD had efforts under way to address the problems highlighted in the internal memorandum and had developed an action plan to track its progress on

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

[2]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.

various human capital, mission, and administrative issues.[3] As requested, this testimony discusses our preliminary observations on the extent to which DHS has (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.

My statement today is based on preliminary analyses from our ongoing review of the CFATS program for a number of congressional committees and subcommittees.[4] We expect to issue a final report on this work in April 2013. To conduct this work, we are reviewing the CFATS statute and regulation;[5] the *National Infrastructure Protection Plan* (NIPP);[6] as well as applicable ISCD policies, processes, and procedures. We are reviewing and analyzing ISCD documents including the web-based tools used to collect security information from facilities, the ISCD risk assessment approach used to determine a facility's risk, and data ISCD collects from facilities to assign them to risk-based tiers. We are also reviewing documents such as the November 2011 internal memorandum and ISCD security plan review policies and procedures. To confirm our understanding of the security plan review process, we are also gathering and analyzing statistics to determine how many security plans have been reviewed, authorized, and approved from program inception through

[3]GAO, *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). This report was summarized in *Critical Infrastructure Protection: Summary of DHS Actions to Better Manage Its Chemical Security Program,* GAO-12-1044T (Washington D.C. Sept. 20, 2012).

[4]These committees and subcommittees include the Senate Committees on Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; the Judiciary; and Environment and Public Works, Subcommittee on Superfund, Toxics, and Environmental Health; as well as the House Committees on Appropriations, Subcommittee on Homeland Security; Homeland Security; Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies; Energy and Commerce; and Energy and Commerce, Subcommittee on Environment and the Economy. Two individual Members of Congress are also requesters for this work.

[5]Throughout this statement, we used the terms "regulation" or "rule" interchangeably when referring to the CFATS regulation.

[6]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS updated the NIPP in January 2009 to include resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). The NIPP sets forth the risk management framework for the protection and resilience of the nation's critical infrastructure.

December 2012. Regarding communicating and working with facilities to improve security, we contacted officials representing 15 trade associations with members regulated by CFATS to obtain their perspectives on DHS efforts to work with facility owners and operators.[7] Out of these 15 associations, 11 responded, and the information we obtained from them 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 assessed the reliability of the data we used for this statement and found that the data were sufficiently reliable for the purposes of this statement. We also interviewed ISCD officials responsible for overseeing the CFATS program to confirm our understanding of the documents and data provided. We shared the information in this statement with DHS officials and incorporated its comments where appropriate. We are conducting our work in accordance with generally accepted government auditing standards.

Background

Section 550 of the DHS appropriations act for fiscal year 2007[8] 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.[9] The CFATS rule was published in April 2007,[10] and appendix A to the rule, published in November 2007, listed 322 chemicals of interest and the screening

[7]We selected these 15 trade associations because they are listed in the 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.

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

[9]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.

[10]72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified at 6 C.F.R. pt. 27).

threshold quantities for each.[11] 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 final 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. During fiscal year 2012, ISCD was authorized 242 full-time-equivalent positions.

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.[12] Once ISCD estimates a risk score based on these models, it assigns the facility to a final tier.

[11]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.

[12]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 Assigned Thousands of Facilities to Tiers, but ISCD's Approach to Risk Assessment Does Not Reflect All Risk Elements

ISCD Has Tiered Thousands of High-Risk Chemical Facilities and Resolved Some Problems Using Its Risk Assessment Approach to Assign Tiers

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.[13] 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.[14]

Over the last 2 years, ISCD has identified problems with the way the release chemicals model assigns chemical facilities to tiers and has taken or begun to take action to address those problems. In February 2011, ISCD found that some chemical facilities had been placed in an incorrect final tier because this model included incorrect data about the release of high-risk chemicals of interest. In June 2011, ISCD officials adjusted the model, which resulted in lowering the tier for about 250 facilities, about 100 of which were subsequently removed from the CFATS program. In October 2012, ISCD officials stated that they had uncovered another defect that led the model to exclude population density calculations for about 150 facilities in states or U.S. territories outside the continental United States, including Alaska, Hawaii, Puerto Rico, and Guam. In

[13]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.

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

February 2013, ISCD officials said that they had made adjustments to the model to resolve this issue and do not expect any facilities' tier will change due to this issue.

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

Our preliminary analyses indicates that the tiering approach ISCD uses to assess risk and assign facilities to final tiers does not consider all of the elements of risk associated with a terrorist attack involving certain chemicals. According to the 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 does not fully consider all of the core criteria or components of a risk assessment, as specified by the NIPP, nor does 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.[15] Our review of ISCD's risk assessment approach and discussions with ISCD officials shows that the approach is currently limited to focusing on one component of consequences—human casualties associated with a terrorist attack involving a chemical of interest—and does 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 stated that they had 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 the initial

[15]6 C.F.R. §§ 27.105, .205.

stages, with an expected completion date of June 2014.[16] ISCD officials added they are uncertain about how Sandia's efforts will affect their risk assessment approach.

- *Threat.* ISCD's risk assessment approach is also not consistent with the NIPP because it does 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 site vulnerability as part of the final determination of a facility's tier.[17] Our review of the models and discussions with ISCD officials shows that (1) ISCD is inconsistent in how it assesses 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 does not consider threat for the approximately 90 percent of facilities that are tiered because of the risk of theft or diversion; and (2) ISCD does not use current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage. ISCD did not have documentation to show why threat had not been factored into the formula for approximately 90 percent of facilities tiered because of the risk of theft or diversion. However, ISCD officials pointed out that the cost of adding a threat analysis for these facilities might outweigh the benefits of doing so. ISCD officials said that given the complexity of assessing threat for theft or diversion, they are considering reexamining their approach. ISCD officials also said that they are exploring how they can use more current threat data for the 10 percent of facilities tiered because of the risk of release or sabotage.

- *Vulnerability*. ISCD's risk assessment approach is also not consistent with the NIPP because it does not consider vulnerability when developing risk scores. According to the NIPP, risk assessments should identify vulnerabilities, describe all protective measures, and

[16]Sandia National Laboratories is a Federally Funded Research and Development Center of the Department of Energy that provides independent consulting services to DHS with regard to modeling, simulation, and analysis of risk-based assessments among other things.

[17]6 C.F.R. §§ 27.215, .220.

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 risk-based tiering process.[18] This 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. Our review of the risk assessment approach and discussions with ISCD officials shows that the security vulnerability assessment contains numerous questions aimed at assessing vulnerability and security measures in place but the information is 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. As a result, 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, but at the latter stages of the CFATS regulatory process particularly with regard to the development and approval of the facility site security plan.

ISCD Has Begun to Take Actions to Examine How Its Approach Could Be Enhanced

Our preliminary work indicates that ISCD has begun to take some actions to examine how its risk assessment approach can be enhanced. For example, in addition to engaging Sandia National Laboratories to develop the framework for assessing economic consequences previously discussed, ISCD has commissioned a panel of subject matter experts to examine the strengths and weaknesses of its current risk assessment approach. ISCD officials stated that the panel's work is intended to focus on whether ISCD is heading in the right direction, and they view it as a preliminary assessment. According to ISCD's task execution plan, the panel is to provide actionable recommendations on potential improvements to the CFATS models, but the panel is not to develop alternative CFATS models or formally validate or verify the current CFATS risk assessment approach—steps that would analyze the structure of the models and determine whether they calculate values correctly. In February 2013, after the panel was convened, ISCD officials stated that they provided information to the panel about various issues that they might want to consider, among them, (1) how to address

[18] 6 C.F.R. § 27.220.

vulnerability in the models given ISCD concerns about data quality, and (2) what the appropriate variables to use, if any, are for threats associated with theft or diversion, as discussed earlier.

We believe that ISCD is moving in the right direction by commissioning the panel to identify the strengths and weaknesses of its risk assessment approach, and the results of the panel's work could help ISCD identify issues for further review and recommendations for improvement. Given the critical nature of ISCD's risk assessment approach in laying the foundation for further regulatory steps in improving facility security—such as the development and approval of facility site security plans—it is important that its approach for assigning facilities to tiers is complete within the NIPP risk management framework and the CFATS rule. Once ISCD's develops a more complete approach for assessing risk it would then be better positioned to commission an independent peer review. In our past work, we reported that peer reviews are a best practice in risk management[19] and that independent expert review panels can provide objective reviews of complex issues.[20] Furthermore, the National Research Council of the National Academies has recommended that DHS improve its risk analyses for infrastructure protection by validating the models and submitting them to external peer review.[21] As we have previously reported, 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 process.[22] We will continue to monitor and assess ISCD's efforts to examine its risk assessment approach through our

[19]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.

[20]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).

[21]National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*. (Washington, D.C. 2010).

[22]See GAO-12-14 and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T (Washington D.C.: Mar. 31, 2004).

ongoing work and consider any recommendations needed to address these issues.

ISCD 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

Our preliminary work shows that ISCD has 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.[23] The November 2011 internal memorandum that discussed various challenges facing the CFATS program noted that ISCD had not approved any security plans and stated that the process was overly complicated and created bottlenecks. The memorandum stated that revising the process was a top program priority because the initial security plan reviews were conducted using the risk-based standards as prescriptive criteria rather than as standards for developing an overall facility security strategy.[24]

According the ISCD officials, the first revision was called the interim review process, whereby individual reviewers were to consider how layers of security measures met the intent of each of the 18 standards. Under the interim review process, ISCD assigned portions of each facility's plan

[23]6 C.F.R. § 27.210(a)(3), .225.

[24]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.

to security specialists (e.g., cyber, chemical, and physical, among others) who reviewed plans in a sequential, linear fashion. Using this approach, plans were reviewed by different specialists at different times culminating in a quality review. ISCD officials told us that the interim review process was unsustainable, labor-intensive, and time-consuming, particularly when individual reviewers were looking at pieces of thousands of plans that funneled to one quality reviewer.[25] In July 2012, ISCD stopped using the interim review process and began using the current revised process, which entails using contractors, teams of ISCD employees (physical, cyber, chemical, and policy specialists), and ISCD field office inspectors, who are to review plans simultaneously.

ISCD officials said that they believe the revised process for reviewing security plans is 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. They said that, under the revised process, among other things, field inspectors are to work with facilities with the intent of resolving any deficiencies ISCD identifies in their site security plans. They added that this contrasts with past practices whereby ISCD would review the entire plan even when problems were identified early and not return the plan to the facility until the review was complete, resulting in longer reviews. Moving forward, ISCD officials said they intend to measure the time it takes to complete parts of the revised process and have recently implemented a plan to measure various aspects of the process. Specifically, ISCD's *Annual Operating Plan*, published in December 2012, lists 63 performance measures designed to look at various aspects of the site security plan review process—from the point the plans are received by ISCD to the point where plans are reviewed and approved. Collecting data to measure performance about various aspects of the security plan review 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 its progress.

[25]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.

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

ISCD has taken action to improve its security plan review process, but based on our preliminary analysis, it could take years to review the plans of thousands of facilities that have already been assigned a final tier. ISCD hopes to address this by examining how it can further accelerate the review process. According to ISCD officials, between July 2012 and December 2012, ISCD had approved 18 security plans, with conditions.[26] ISCD officials told us that, moving forward, they anticipate that the revised security plan review process could enable ISCD to approve security plans at a rate of about 30 to 40 a month.

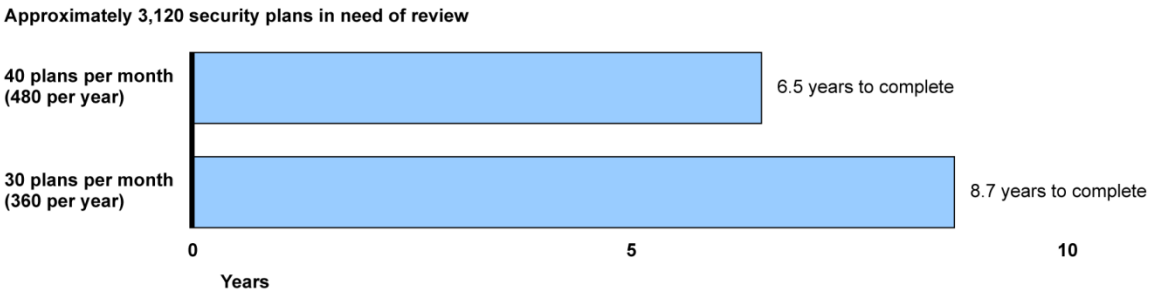
Using ISCD's estimated approval rate of 30 to 40 plans a month, our preliminary analysis indicates that it could take anywhere from 7 to 9 years to complete reviews and approvals for the approximately 3,120 plans[27] submitted by facilities that have been final-tiered that ISCD has not yet begun to review.[28] Figure 1 shows our 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.

[26]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.

[27]ISCD data show that 380 security plans have started the review process and are at different phases of review.

[28]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.

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



Source: GAO.

It is important to note that our 7- to 9-year preliminary estimate does not include other activities central to the CFATS mission, either related to or aside from the security plan review process. In addition, our estimate does not include developing and implementing the compliance inspection process, which occurs after security plans are approved and is intended to ensure that facilities that are covered by the CFATS rule are compliant with the rule, within the context of the 18 performance standards. According to ISCD officials, they are actively exploring ways to expedite the speed with which the backlog of security plans could be cleared, such as potentially leveraging alternative security programs, reprioritizing resources, and streamlining the inspection and review requirements. ISCD officials added that they plan to complete authorizations inspections and approve security plans for tier 1 facilities by the first quarter of fiscal year 2014 and for tier 2 facilities by the third quarter of fiscal year 2014.

ISCD Has Increased Its Efforts to Communicate and Work with Facilities, but Does Not Solicit Systematic Feedback on Effectiveness of Its Outreach

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

Our preliminary work shows that ISCD's efforts to communicate and work with owners and operators to help them enhance security at their facilities have increased since the CFATS program's inception in 2007, particularly in recent years. Since 2007, ISCD has 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. From fiscal years 2007 through 2009, most of ISCD's communication efforts entailed outreach with owners and operators and stakeholders through presentations to familiarize them with CFATS; field visits with federal, state, and local government and private industry officials; and compliance assistance visits at facilities that are intended to assist facilities with compliance or technical issues. By 2010 and in subsequent years, ISCD had revised its outreach efforts to focus on authorization inspections during which inspectors visited facilities to verify that the information in their security plans was accurate and complete, and other outreach activities including stakeholder outreach.[29]

[29]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 it operates on a contract basis by the Oak Ridge National Laboratory. According to ISCD, from April 2007 through July 2012, the Help Desk responded to nearly 80,000 user inquires, submitted via telephone, e-mail and fax. We did not review the quality of the responses provided through the help desk function or assess the qualifications of the staff responding to user inquires because doing so was outside of the scope of this review.

However, analysis of industry trade associations' responses to questions we sent them about the program shows mixed views about ISCD's efforts to communicate with owners and operators through ISCD outreach efforts. For example, 3 of the 11 trade associations that responded to our questions indicated that ISCD's outreach program was effective in 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.[30]

ISCD Seeks Informal Feedback, but Does Not Solicit Systematic Feedback on the Effectiveness of Its Outreach Efforts

Our preliminary results indicate that ISCD seeks informal feedback on its outreach efforts but does not systematically solicit feedback to assess the effectiveness of outreach activities,[31] and it does not have a mechanism to measure the effectiveness of ISCD's outreach activities. Trade association officials reported that in general ISCD seeks informal feedback on its outreach efforts and that members provide feedback to ISCD. Association officials further reported that among other things ISCD has encouraged association members to contact local ISCD inspectors and has hosted roundtable discussions and meetings where members of the regulated community provide feedback, suggest improvements, or make proposals regarding aspects of the CFATS program such as site security plans, alternative security programs, and gasoline storage site risks. Furthermore, according to ISCD officials, while feedback is solicited from the regulated community generally on an informal basis, inspectors and other staff involved in ISCD's outreach activities are not required to solicit feedback during meetings, presentations, and assistance visits, and inspectors are also not required to follow up with the facilities after compliance assistance visits to obtain their views on the effectiveness of the outreach.

[30]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.

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

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. We have previously reported on the benefits of soliciting systematic feedback. Specifically, our prior work on customer service efforts in the government indicates that systematic feedback from those receiving services can provide helpful information as to the kind and quality of services they want and their level of satisfaction with existing services. We will continue to monitor and assess ISCD's efforts to develop a systematic way to solicit feedback through our ongoing work and consider any recommendations needed to address this issue.

Chairman Shimkus, Ranking Member Tonko, 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.

GAO Contact 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.