United States Government Accountability Office

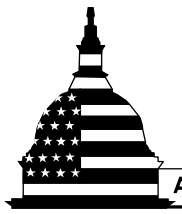
GAO

Report to Congressional Requesters

April 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened



G A O

Accountability * Integrity * Reliability

GAO-13-353

April 2013

CRITICAL INFRASTRUCTURE PROTECTION

DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-353, a report to congressional requesters.

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. A November 2011 ISCD internal memorandum raised concerns about ISCD's ability to fulfill its mission.

GAO assessed 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. 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

GAO recommends 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.

View GAO-13-353. For more information, contact Steve Caldwell at (202) 512-9610 or 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 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 has begun to take some actions to examine how its risk assessment approach can be enhanced, including commissioning a panel of experts to assess the current approach, identify strengths and weaknesses, and recommend improvements. ISCD will need to incorporate the various results of these efforts to help them ensure that the revised risk assessment approach includes all elements of risk. After ISCD has incorporated all elements of risk into its assessment 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.

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 to measure differences. 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. 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 which means that 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 reprioritizing resources and streamlining inspection requirements.

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. 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.

Contents

Figures

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 5, 2013

Congressional Requesters

Facilities that produce, use, or store hazardous chemicals could be of particular interest to terrorists who are intent on using toxic chemicals to inflict mass casualties in the United States. These chemicals could be released from a facility to cause harm to surrounding populations, could be stolen and used as chemical weapons or as their precursors (the ingredients for making chemical weapons), or stolen and used to build an improvised explosive device. The Department of Homeland Security (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.[2] In 2007, DHS established the Chemical Facility Anti-Terrorism Standards (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 these chemical facility security regulations. Within NPPD, the Office of Infrastructure Protection (IP), through its Infrastructure Security Compliance Division (ISCD), oversees the CFATS 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 December 2011, this memorandum, prepared by the then ISCD Director, was leaked to the national media, raising concerns about the management of the program.

[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. In this report, we use the term "chemical facilities" to cover different types of facilities regulated under CFATS. This can include facilities that manufacture chemicals; those that use certain chemicals to manufacture products, such as microchips; or education facilities that use chemicals for research purposes, among others.

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. 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 various human capital, mission, and administrative issues.[3] We found that ISCD appeared to be heading in the right direction, but it was too early to tell if individual action items were having their desired effect because ISCD was in the early stages of implementing them and had not yet established performance measures to assess results. We recommended that ISCD explore opportunities to develop such measures, where practical. ISCD agreed with our recommendation and in response, developed an operating plan that includes information on how ISCD plans to measure performance. We also noted that some of the action items such as developing an appropriate information technology platform to support inspection activities would require a longer-term effort by ISCD. You asked us to follow up on ISCD's efforts to address various mission issues such as a security plan review process that, according to ISCD, was overly complicated and difficult to implement. Specifically, this report discusses the extent to which DHS has

- assigned chemical facilities to risk-based tiers and assessed its approach for doing so,
- revised the process used to review security plans, and
- communicated and worked with facilities to help improve security.

To meet our objectives, we reviewed the CFATS statute and regulation (or rule),[4] as well as ISCD policies, processes, and procedures that were in place from CFATS program inception to date. Regarding assigning

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

chemical facilities to risk-based tiers, we reviewed and analyzed 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, policies and procedures on risk-based tiering, among others; and data ISCD collects from facilities to make tiering determinations. We assessed the reliability of the data collected and found that the data were sufficiently reliable for the purposes of this report. We compared our analysis against various criteria such as the CFATS statute and rule; the National Infrastructure Protection Plan (NIPP), which sets forth the risk management framework for the protection and resilience of the nation's critical infrastructure;[5] and risk modeling best practices as outlined by the National Academy of Sciences to determine if ISCD's risk assessment approach comports with these criteria[6] and if not, where gaps exist. We also reviewed documents related to ISCD's ongoing efforts to review its risk assessment approach including the statement of objectives, task execution plan, and terms of reference and compared these documents to the criteria for peer review as laid out by the National Academy of Sciences as well as our prior work on peer reviews. [7]

Regarding ISCD's revisions to the security plan review process, we reviewed documents such as the November 2011 internal memorandum, DHS's Risk-Based Performance Standards Guidance, and ISCD security plan review policies and procedures, among others. To confirm our understanding of the security plan review process, we also gathered and analyzed statistics pertinent to the process to determine how many security plans had been reviewed, authorized, and approved from

[5]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). Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

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

[7]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, 2010) and 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).

program inception to date. We did not include the facility compliance inspection process (which is based on the results of the approved security plans) because ISCD began notifying facilities that their security plans were approved in December 2012.

Regarding communicating and working with facilities to improve security, we contacted officials representing 15 trade associations with members regulated by CFATS and who participated in the Chemical Sector Coordinating Council to get their perspectives on DHS efforts to work with facility owners and operators.[8] Out of the 15 trade associations we contacted, 11 responded and the information we obtained from them is not generalizable to the universe of chemical facilities covered by CFATS. However, the information we obtained from them provides insights into DHS efforts to perform outreach and seek feedback on the implementation of the CFATS rule. For all our objectives, we interviewed ISCD officials responsible for overseeing the CFATS program to confirm our understanding of the documents and data provided. Appendix I discusses our scope and methodology in greater detail.

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.

Background

The CFATS program is intended to secure the nation's chemical infrastructure by identifying and protecting high-risk chemical facilities. Section 550 of the DHS appropriations act for fiscal year 2007 requires

[8]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 is 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. According to the NIPP, a Sector Coordinating Council is the principal entity under which owners and operators of critical infrastructure can coordinate with the government on a wide range of protection activities and issues. The Chemical Sector Coordinating Council represents owners and operators of chemical facilities.

DHS to issue regulations establishing risk-based performance standards[9] for the security of facilities that the Secretary determines to present high levels of security risk.[10] The CFATS rule was published in April 2007[11] and Appendix A to the rule, published in November 2007, listed 322 chemicals of interest and the screening threshold quantities amount for each.[12]

ISCD has direct responsibility for implementing DHS's CFATS rule, including assessing risks and identifying high-risk chemical facilities, promoting effective security planning, and ensuring that high-risk facilities meet the applicable risk-based performance standards through site security plans approved by DHS. ISCD is managed by a Director and operates five branches that are, among other things, responsible for (1) information technology operations; (2) policy and planning; (3) providing compliance and technical support; (4) inspecting facilities and enforcing CFATS regulatory standards; and (5) managing logistics, administration, and chemical security training.[13] From fiscal years 2007 through 2012, DHS dedicated about $442 million to the CFATS program. In fiscal year 2012, DHS was authorized 242 full-time equivalent positions.

The CFATS Rule and Process

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

[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 of the applicable areas.

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

[11]72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified at 6 C.F.R. pt. 27).

[12]72 Fed. Reg. 65,396 (Nov. 20, 2007). According to DHS, CFATS covers facilities that manufacture chemicals as well as 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.

[13]ISCD receives business support from NPPD and IP for services related to human capital management and training, budget and finance, and acquisitions and procurement.

Assessment Tool (CSAT)—a web-based application through which owners and operators of chemical facilities provide information about the facility.[14] 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.[15] 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.[16] 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.[17] 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.[18] 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.[19]

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

[14]6 C.F.R. § 27.200(b).

[15]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.

[16]6 C.F.R. § 27.205(a).

[17]6 C.F.R. § 27.220(a), (c).

[18]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).

[19]6 C.F.R. § 27.220(b), (c).

a site security plan.[20] 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.[21] 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.[22] If the facility fails to correct the deficiencies, DHS may disapprove the plan.[23] Following approval, DHS may conduct further inspections to determine if the facility is in compliance with its approved security plan.[24] Figure 1 illustrates the CFATS regulatory process.

[20]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.

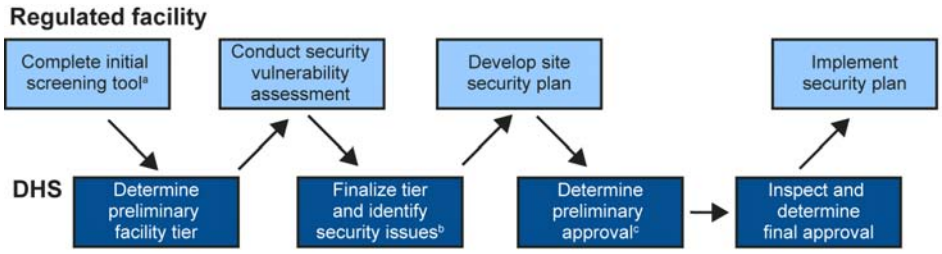
[21]6 C.F.R. § 27.225.

[22]According to 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.

[23]6 C.F.R. § 27.245.

[24]6 C.F.R. § 27.250.

Figure 1: 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.

ISCD's Approach to Risk Assessment

ISCD uses a risk assessment approach during the early stages of the regulatory process to develop risk scores to assign chemical facilities to a final tier. 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). The ISCD 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 of interest listed in Appendix A of the CFATS rule. 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. 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 Does Not Reflect All Risk Elements

Since 2007, ISCD has assigned about 3,500 high-risk chemical facilities to final tiers and has taken action to identify and address problems with its risk-tiering approach. However, ISCD's risk-tiering approach does not reflect all elements of risk. Specifically, ISCD is to assess risk using estimates of the consequences, threat, and vulnerability associated with a terrorist attack, but ISCD does not consider key elements of risk, such as economic consequences or facility vulnerability consistent with the NIPP and the CFATS rule. ISCD recognizes that its tiering approach is not complete and continues to mature and has begun to take actions to assess its approach, including commissioning an expert panel.

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.[25] 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. In addition, about 900 of the 4,400 facilities had been assigned to preliminary tiers and were to be assigned a final tier once ISCD processed data from the facility using ISCD's risk assessment approach. ISCD officials noted that the number of tiered facilities and their individual tiers is likely to be fluid over time as changes in chemical holdings, production, processes, storage methods, or use occur. Table 1 shows the number and percentage of facilities assigned a final tier as of January 2013. [26]

[25]According to ISCD officials, approximately 35,600 facilities were not considered high risk because after preliminary evaluation using the Top Screen, 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.

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

Table 1: Number and Percent of Facilities Assigned a Final Tier as of January 2013

	Number	Percent
Tier 1	117	3.4
Tier 2	406	11.6
Tier 3	1,040	29.8
Tier 4	1,932	55.3
Total	**3,495**	**100.0**

Source: GAO analysis of Infrastructure Security Compliance Division data.

Note: Percentages do not add to 100 because of rounding.

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 managers were notified by contracting officials responsible for running the model 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, lowering the tier for about 250 facilities, about 100 of which were subsequently removed from the CFATS program. In September 2012, ISCD officials stated that they were confident that the adjustment helped make this model more accurate.

However, in October 2012, ISCD officials stated that they had discovered another anomaly that they were working to correct. Specifically, ISCD officials said that they had uncovered a 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 December 2012, ISCD officials said that they had made adjustments to the model to resolve this issue. They added that they expected that once data from the approximately 150 facilities were assessed, no more than 11 of the approximately 150 facilities would be affected by a change to their tier. ISCD officials said that as of February 2013, upon further examination, they expect that about 2 facilities will be affected. However, those two facilities were already tiered for other chemicals covered by CFATS, and ISCD officials did not expect those facilities' respective tiers to change.

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

ISCD has tiered thousands of facilities using its current risk assessment approach, but ISCD's risk assessment approach is not mature because it does not consider key elements of risk from the NIPP and the CFATS rule. 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

ISCD's risk assessment approach does not currently conform to the NIPP and is not consistent with the CFATS rule because it does not yet fully consider consequence criteria when assessing risk associated with a terrorist attack. 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. Like the NIPP, 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.[27]

Our review of ISCD's risk assessment approach and discussions with ISCD officials showed 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 told us that, at the inception of the CFATS program, they did not have the capability to collect or process all of the economic data needed to calculate the associated risks and they were not positioned to gather all of the data needed. They said that they collect basic economic data as part of the initial screening process in the CSAT; however, they would need to modify the current tool to collect more sufficient data. This contrasts with other DHS components, like the U.S. Coast Guard and the Transportation

[27]6 C.F.R. §§ 27.105, .205.

Security Administration, which have gathered and assessed economic data as part of some critical infrastructure risk assessment efforts.

ISCD officials stated that they have begun to have discussions with other DHS components, like the U.S Coast Guard, about their approach to risk assessment. They also said that they recognize that the economic consequences part of their risk-tiering approach will require additional work before it is ready to be introduced. They noted that the preamble to the November 2007 CFATS rule stated that they would defer incorporating economic criticality until a later date. In September 2012, ISCD officials told us 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 stages, with an expected completion date of June 2014.[28] ISCD officials added they are uncertain about how Sandia National Laboratories' 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. Like the NIPP, the CFATS rule requires that, as part of site vulnerability assessment process, 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.[29] Our review of the models and discussions with ISCD officials showed 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.

[28]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.

[29]6 C.F.R. §§ 27.215, .220.

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, they pointed out that the cost of adding a threat analysis for these facilities might outweigh the benefits of doing so because it may not provide the increased specificity and level of details to justify the cost. Officials further explained that the model assumes that a terrorist would remove the chemical of interest and use it offsite and ISCD cannot predict where a chemical of interest would be used as a result of theft or diversion. Nonetheless, it is inconsistent for ISCD to not consider threat for the theft or diversion risk model, given that the assumptions about an attack are similar to those considered under the sabotage model—that is, both models assume that a terrorist would use a chemical of interest at an offsite, undisclosed location. This extra level of specificity would be useful for ISCD's overall risk assessment efforts given that about 90 percent of facilities are regulated because of the theft or diversion security issue. ISCD officials said that given the complexity of assessing threat for theft or diversion, they are considering reexamining their approach.

Regarding the other 10 percent—facilities tiered because of the risk of release or sabotage—ISCD documents showed that both models consider threat data based primarily on the location of the facility. Nonetheless, ISCD could use more current data to estimate threat among these facilities. Our review showed that ISCD is using 5-year-old threat data based on metropolitan statistical areas (MSA) to estimate threat for those facilities even though these data are updated annually by DHS for purposes of the Urban Areas Security Initiative program.[30] ISCD officials said that they were unaware that threat data they were using were out of date and said they would explore the feasibility of using updated threat scores. Current threat data would provide a more complete and accurate threat profile for release or sabotage and might aid in ISCD's overall risk assessment efforts.

Vulnerability

ISCD's risk assessment approach is also not consistent with the NIPP because it does not consider vulnerability when developing risk scores.

[30]The Urban Areas Security Initiative program is a Homeland Security Grant Program which is intended to provide funding to address the unique planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assist them in building an enhanced and sustainable capacity to prevent, protect against, mitigate, respond to, and recover from acts of terrorism.

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 risk-based tiering process.[31] 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 performances standards.

Our review of the risk assessment approach and discussions with ISCD officials showed that the security vulnerability assessment—the primary CSAT application ISCD uses to assess risk—contains numerous questions aimed at assessing vulnerability and security measures in place. These include questions about the accessibility of the facility to an attacker, the capability of the security force to respond to an attack, and security controls related to potential cyber attacks. However, although facilities are required to respond to these questions, ISCD officials told us that they have opted not to use the data facilities provide because it is "self-reported" data—data that are not validated by ISCD—and ISCD officials have observed that facility owners and operators tend to either overstate or understate some of the vulnerability information provided; thus making it not useful for tiering purposes. ISCD officials agreed that the risk assessment approach does not assess differences in vulnerability from facility to facility and location to location because it does not use any vulnerability data. 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, but primarily at the latter stages of the CFATS regulatory process particularly with regard to the development and approval of the facility site security plan and the inspection process. With regard to site security plans, ISCD officials stated that even though facility data are not currently used to tier facilities based on their response in the security vulnerability assessment, they view the responses as valuable because they prompt facilities' thinking about vulnerability before they prepare their site security plan or alternative security program. Regarding inspections, ISCD officials stated

[31] 6 C.F.R. § 27.220.

that they believe that once security plans are authorized and approved, the inspection process could enable ISCD to assess facilities' vulnerabilities and gauge their progress mitigating those vulnerabilities. Because ISCD has completed a limited number of authorization inspections (56 as of December 2012), it is too early to tell how they plan to use this self-reported vulnerability information. However, ISCD officials indicated that it might be used to help make decisions about the use of inspection resources, especially since they do not anticipate retiering facilities based on their efforts to mitigate risk.

ISCD Has Begun to Take Actions to Examine How its Approach Could be Enhanced and Could Take Additional Steps to Help Ensure That it is Complete and Validated

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 discussed earlier, ISCD has commissioned a panel of subject matter experts to examine the strengths and weaknesses, if any, 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 objectives of this assessment are to (1) convene a panel of subject matter experts involved in chemical safety and security, (2) hold one or more working group meetings focused on assessing and providing feedback on the current models and (3) provide a report on the strengths, weaknesses, and issues on the current models. The plan calls for the panel to provide actionable recommendations on potential improvements to the CFATS models, but the panel is not to develop alternative CFATS models nor 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. ISCD officials stated that they believe that the review process would include some steps to assess whether the models are methodologically sound and reliable. In February 2013, after the panel was convened, ISCD officials also stated that they provided information to the panel about various issues that they might want to consider, among them (1) how to address 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.

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. The results of the

panel's efforts represent one piece of information ISCD will have to consider, moving forward, to ensure that the risk assessment approach is complete within the context of the NIPP risk management framework and the CFATS rule. For instance, in addition to any recommendations coming out of the panel's work, the development of a mature risk assessment approach would require that ISCD consider and act upon the results of Sandia National Laboratories work on economic consequences. Likewise, ISCD would need to consider the issues we identified, such as not using up-to-date threat data, or how vulnerability could be used in the final tiering process.

ISCD will need to develop an overall plan designed to incorporate the results of these various efforts to revise and enhance its risk assessment approach to fully address each of the components of risk—consequences, threat, and vulnerability—to better align them with the NIPP and the CFATS rule. A plan, complete with milestones and time frames, is consistent with standard practices for project management, which state that managing a project involves, among other things, developing a timeline with milestone dates to identify points throughout the project to reassess efforts under way to determine whether project changes are necessary.[32] ISCD would then be better situated to provide a more complete picture of its approach for developing and completing its review of steps needed to address each component of ISCD's risk assessment approach and actions needed to make it fully conform to the NIPP and the CFATS rule. It also would provide ISCD managers and other decision makers with insights into (1) ISCD's overall progress and (2) a basis for determining what, if any, additional actions need to be taken.

In addition, given the significant consequences of a terrorist attack on a chemical facility, after ISCD completes these actions, commissioning an independent peer review to assess its revised risk assessment approach, including a complete verification and validation of the models would help ensure that the revised model is sound and facilities are appropriately tiered. In our past work, we reported that peer reviews are a best practice

[32]Project Management Institute, *The Standard for Program Management©*, (Pennsylvania, 2013).

in risk management[33] and that independent expert review panels can provide objective reviews of complex issues.[34] We reported that peer reviews should, among other things, address the structure of the model, the types and certainty of the data, and how the model is intended to be used. 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.[35] According to the National Research Council of the National Academies, peer reviews should include validation and verification to ensure that the structure of the models is both accurate and reliable.

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.[36] Thus, a peer review that is commissioned after ISCD revises its approach and incorporates all of the elements of risk would enable peer reviewers to consider a more complete risk assessment approach and provide the opportunity to fully verify and validate it. After ISCD has developed a more mature risk assessment approach, a subsequent 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.

[33]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.

[34]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).

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

[36]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).

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

ISCD has revised its site security plan review process to address concerns expressed by ISCD managers that the original process was overly complicated and included bottlenecks that slowed the review time. ISCD officials said that they believe the current security plan review process, implemented in July 2012, is an improvement over the prior versions. However, they did not collect or track data on the prior review processes, so the improvement between the previous review processes and the current process cannot be measured. Going forward, ISCD has recently implemented a plan to measure various aspects of the process, but it will take time before ISCD can establish baseline measures. Nonetheless, given the rate at which ISCD intends to review and approve security plans, we estimate that it could take about 7 to 9 years to complete reviews of plans for approximately 3,120 facilities that, as of January 2013, had been assigned a final tier but had not yet had their security plans reviewed and approved.

ISCD Revised Its Security Plan Review Process because of ISCD Managers' Concerns

ISCD has made various revisions to its security plan review process. 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 they will address applicable risk-based performance standards.[37] The November 2011 internal memorandum that discussed various challenges facing the program noted that ISCD had not approved any security plans and stated that the process was overly complicated, did not leverage ISCD's resources, and created bottlenecks. In addition, the memorandum stated that revising the process was a top program priority because the initial security plan reviews were conducted in a manner inconsistent with the spirit and intent of the CFATS authorizing legislation—that is, plan reviewers used the risk-based standards as prescriptive criteria rather than as standards for developing an overall facility security strategy.[38] According to ISCD, the initial reviews were

[37]6 C.F.R. § 27.210(a)(3), .225.

[38]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. 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.

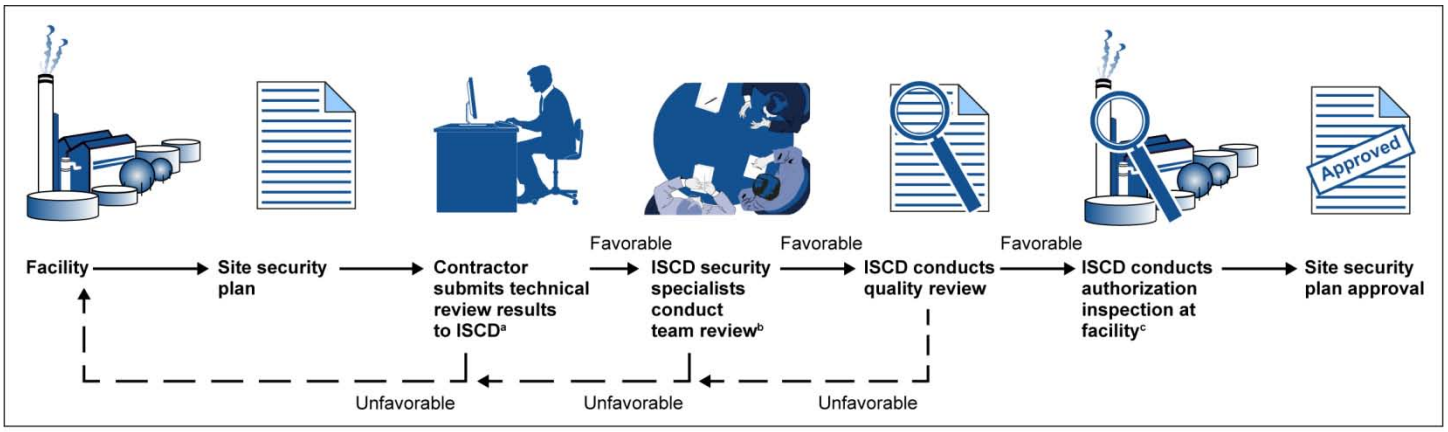
conducted using the 18 risk-based standards as prescriptive criteria because ISCD had not developed guidance for reviewers of facility plans to use when considering the merits of those plans. ISCD officials told us that they had been working on a solution prior to the internal memorandum being finalized in November 2011. They also pointed out that the action plan that was intended to address the challenges outlined in the memorandum, developed in early 2012, included an action item devoted to improving the security plan review process.

ISCD has implemented two revisions to the security plan review process since October 2011. According the ISCD officials, the first revision was called the interim review process, which was intended to be a "holistic" review whereby individual reviewers were to consider how layers of security measures met the intent of each of the 18 standards. This was a departure from the original review process which generally used the performance standards as specific criteria. Under the interim process, ISCD assigned portions of each facility's plan 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 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.[39]

In July 2012, ISCD stopped using the interim process and began using the revised review process. The current process entails using contractors, teams of ISCD employees (physical, cyber, chemical, and policy specialists), and ISCD field office inspectors who are to review plans simultaneously using the holistic approach developed earlier. Figure 2 shows the revised security plan review process as of July 2012.

[39]Using the interim 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.

Figure 2: Infrastructure Security Compliance Division (ISCD) Site Security Plan Review Process as of July 2012



Source: GAO; Art Explosion (clip art).

Notes: When the review of a plan results in an unfavorable determination, the plan is to be returned to the facility and ISCD is to schedule a compliance assistance visit to discuss the reasons for the unfavorable determination with representatives at the facility and present options for the facility's consideration on how to appropriately revise the security plan. The facility is to make changes to the plan at its discretion and resubmit it to ISCD at the point in the process where the unfavorable determination was made.

[a]Contractors conduct the technical review and provide input to ISCD staff who make the decision whether or not the security plan receives a favorable or unfavorable review.

[b]The team that reviews the security plans includes various types of security specialists including physical security, cyber, chemical, policy, and compliance specialists, as well as field offices inspectors.

[c]During an authorization inspection, inspectors can determine that the security measures in place at the facility are not what was presented in the plan and recommend that changes be made to the plan before it is approved. If this occurs, the facility is to edit the plan. Any changes to the plan made at this point in the process are to be reviewed by ISCD officials before the plan is approved.

ISCD Did Not Measure Improvements, but Plans to Measure the Revised Review Process Moving Forward

ISCD officials said that they believe the revised security plan review process is a "quantum leap" forward, but did not capture data that would enable them to measure how, if at all, the new process is more efficient (i.e., less time-consuming) than the former processes. ISCD officials explained that one of the more time-saving beneficial aspects of the new process involves field inspectors interacting with the facilities when the review of the security plan results in an unfavorable outcome. Now, when ISCD identifies a security plan that contains deficiencies, such as missing or unclear information about a security measure, the plan is to be immediately returned to the facility and ISCD is to schedule a compliance assistance visit whereby field inspectors work with the facility to resolve

any issues identified. According to ISCD officials, this approach contrasts with the past practices whereby ISCD would continue to 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.

Officials also noted that by using the revised process, ISCD has realized the value of (1) moving from a single person reviewing every plan sequentially to a team approach, and (2) understanding that security plans do not have to be perfect in order to issue authorization letters and conduct authorization inspections. Regarding the latter, ISCD officials noted that ISCD has begun issuing authorization letters with conditions to inform facilities that their plans provide sufficient information to schedule an inspection. For example, one authorization letter noted that ISCD had not yet determined whether or not the plan satisfied the cyber security risk-based performance standard, and stated that additional information would be gathered during the authorization inspection.

Also, when the revised process was implemented in July 2012, 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.[40] ISCD believes issuing authorization letters with conditions, rather than waiting until all conditions are met, enables inspectors to visit facilities sooner so that ISCD can approve plans more quickly.

Moving forward, ISCD intends to measure the time it takes to complete parts of the new process and has 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

[40]Personnel surety is one of the CFATS performance standards. Accordingly, DHS plans to require facilities to perform background checks on and ensure appropriate credentials for facility personnel and as appropriate, visitors with unescorted access to restricted areas or critical assets. DHS plans to check for terrorist ties by comparing certain employee information with its terrorist screening database. DHS's plans to require facilities to collect these data had been submitted to the Office of Management and Budget (OMB) for review in connection with the Paperwork Reduction Act. However, DHS had withdrawn its Paperwork Reduction Act request and stated that OMB is not considering the request at this time. As of January 2013, ISCD has not refiled its Personnel Surety Information Collections Request with OMB.

review process—from the point the plans are received by ISCD to the point where plans are reviewed and approved. For example, ISCD plans to collect data on (1) the percentage of facilities with authorization inspections completed within 90 days of security plan authorization for tier 1 and 2 facilities and within 120 days of security plan authorization for tier 3 and 4 facilities, and (2) the number of high-risk facilities in total and by tier that have approved security plans. 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. As of February 2013, ISCD is beginning to gather data at points in the process to establish baselines and measure performance and has a goal of reviewing some of the measures and data associated with them monthly, quarterly, or annually, depending on the measure.

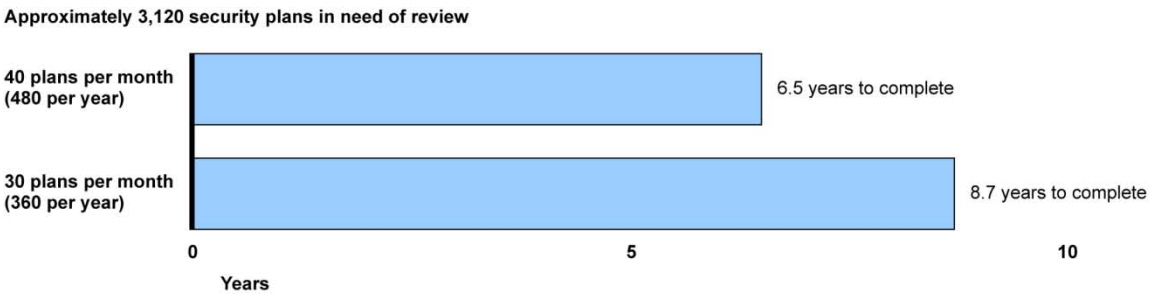
Security Plan Reviews Could Take Years to Complete, but ISCD is Examining How it Can Accelerate the Review Process

ISCD actions to revise its security plan reviews may result in improvements over the prior processes, but it could take years to review plans for thousands of facilities that have been assigned a final tier—a factor which ISCD hopes to address by examining how it can accelerate the review process. According to ISCD officials, between July 2012 and December 2012, ISCD had approved 18 security plans, with conditions such as the aforementioned personnel surety qualification. 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. Furthermore, ISCD officials noted 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. However, ISCD estimates that under a best case scenario the revised review process could take about 6 months to approve a plan—assuming the plan would not have to be sent back to the facility for revision. ISCD estimates further show that under a worst case scenario the revised process could take as long as 20 months to approve a plan—assuming the plan would have to be sent back to the facility for revisions. Regardless, ISCD officials told us that they would likely be able to increase production because staff are overcoming the learning curve associated with the revised process.

Using ISCD's estimated approval rate of 30 to 40 plans a month, we calculated that it could take anywhere from 7 to 9 years to complete

reviews and approvals for the approximately 3,120 plans submitted by facilities that have been final-tiered that ISCD has not yet begun to review.[41] Figure 3 shows the estimated 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 3: Estimate of Number of Years to Approve Security Plans



Source: GAO.

It is important to note that our 7 to 9 year estimate does not include other activities central to the CFATS mission, either related to or aside from the security plan review process. Specifically, our estimate does not include time required to:

- review security plans for about 900 facilities that have yet to be assigned a final tier; and
- review approved security plans to resolve issues relating to personnel surety, which cannot be fully accomplished until after ISCD decides how to conduct the terrorist ties portion of personnel surety.

Finally, our estimate does not include developing and implementing the compliance inspection process, which 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. ISCD officials estimate that the

[41]ISCD data show that 380 security plans have started the review process and are at different phases of review. 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 3rd quarter of fiscal year 2013.

first compliance inspections would commence in September 2013, which means that the CFATS regulatory regime would likely be fully implemented for currently tiered facilities (to include compliance inspections) in 8 to 10 years. According to ISCD officials, they are actively exploring ways to expedite the speed with which the backlog of security plans will be cleared such as potentially leveraging alternative security programs, re-prioritizing 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 and May Have an Opportunity to Systematically Gather Feedback on Its Outreach Efforts

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. The various trade associations representing facility owners and operators who responded to our query on ISCD's outreach had mixed views about the effectiveness of ISCD's efforts to communicate with them over various aspects of the program. Most of the trade associations that responded stated that ISCD seeks and receives informal feedback on its communication efforts, but ISCD stated that it has not developed a systematic approach to solicit feedback to assess the effectiveness of its outreach activities. ISCD is currently developing a strategic communication plan which may create an opportunity for ISCD to explore how it can obtain systematic feedback on its outreach.

ISCD's External Communication Efforts with Facilities have Increased Since 2007

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 and these efforts have increased as the program has matured.[42] 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 them with compliance or technical issues. By 2010 and in subsequent years, ISCD revised its outreach efforts to focus on authorization inspections[43] 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.[44] Table 2 shows the number of outreach activities performed by ISCD from fiscal year 2007 through the first quarter of fiscal year 2013.

[42]As part of the outreach program, ISCD consults with external stakeholders such as private industry and state and local government officials who participate in Sector Coordinating Councils and Government Coordinating Councils, to discuss issues that affect the program and facility owners and operators. Under the NIPP, the sector partnership model encourages critical infrastructure owners and operators to create or identify Sector Coordinating Councils as the principal entities for coordinating with the government. The Government Coordination Council is the government counterpart for each Sector Coordinating Council and comprises representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector.

[43]In fiscal years 2010 and 2011, ISCD also performed pre-authorization inspections at regulated facilities, an activity that is now included with the compliance assistance visits.

[44]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 the CSAT Help Desk (call service center), which it operates on a contract basis by the Oak Ridge National Laboratory (ORNL). The call service center's standard operating procedures state service center representatives answer inbound calls and e-mails from users of the CSAT data collection tools. ISCD reported that from April 2007 through July 2012, the CSAT 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 it was outside of the scope of this review.

Table 2: Number of Outreach Activities Performed by DHS's Infrastructure Security Compliance Division from Fiscal Year 2007 through the First Quarter Fiscal Year 2013

Fiscal year	Compliance assistance visits[a]	Authorization inspections[b]	Stakeholder outreach[c]	Presentations[d]	Field meetings[e]
2007	N/A	N/A	N/A	53	N/A
2008	99	N/A	N/A	244	95
2009	63	N/A	N/A	147	136
2010	226	3	N/A	102	385
2011	595	6	2,644	131	1,124
2012	288	18	1,721	117	2,697
First Quarter 2013	68	35	139	41	485
Total	**1,339**	**62**	**4,504**	**835**	**4,922**

Source: DHS.

Note: N/A represents not available for those fiscal years where ISCD had not collected outreach data.

[a]Compliance assistance visits are visits to regulated or potentially regulated chemical facilities with the goal of providing compliance and technical assistance in the completion of the CSAT registration, Top Screen, security vulnerability assessment, or site security plan. ISCD conducted preliminary authorization inspections in fiscal years 2010 and 2011, which are now included with compliance assistance visits. The latter were visits performed at regulated chemical facilities with the goal to educate the facility on the level of detail that is required within the site security plan in order for the department to adequately review and assess the facility's security posture for compliance with CFATS. For purposes of this analysis, we included ISCD data on preliminary authorization inspections with data on compliance assistance visits.

[b]Authorization inspection are visits to regulated chemical facilities in order to verify that the descriptions listed in the facility's authorized site security plan (or alternative security program) are accurate and complete, and that the equipment, processes, and procedures described are appropriate and function as intended.

[c]Stakeholder outreach refers to meetings at CFATS regulated facilities at which inspectors introduce themselves, meet key facility representatives, provide basic outreach materials, and familiarize themselves with their local regulated community.

[d]Presentations are provided at federal, state, local, or private industry events in which an ISCD representative is asked to provide a presentation or participate on a panel in order to provide CFATS subject matter expertise.

[e]Field meetings are meetings with federal, state, local, or private industry partners in which the inspectors participate to better familiarize themselves with other programs, activities and harmonize with key stakeholders.

According to ISCD officials, the increase in outreach was intended to facilitate the development of site security plans and occurred for various reasons. First, according to ISCD officials, during the early years of the program, regulated facilities did not require as much assistance because they were generally engaged in the development of their Top Screens and security vulnerability assessments. Second, officials said that, as ISCD matured, its ability to track outreach activities improved when

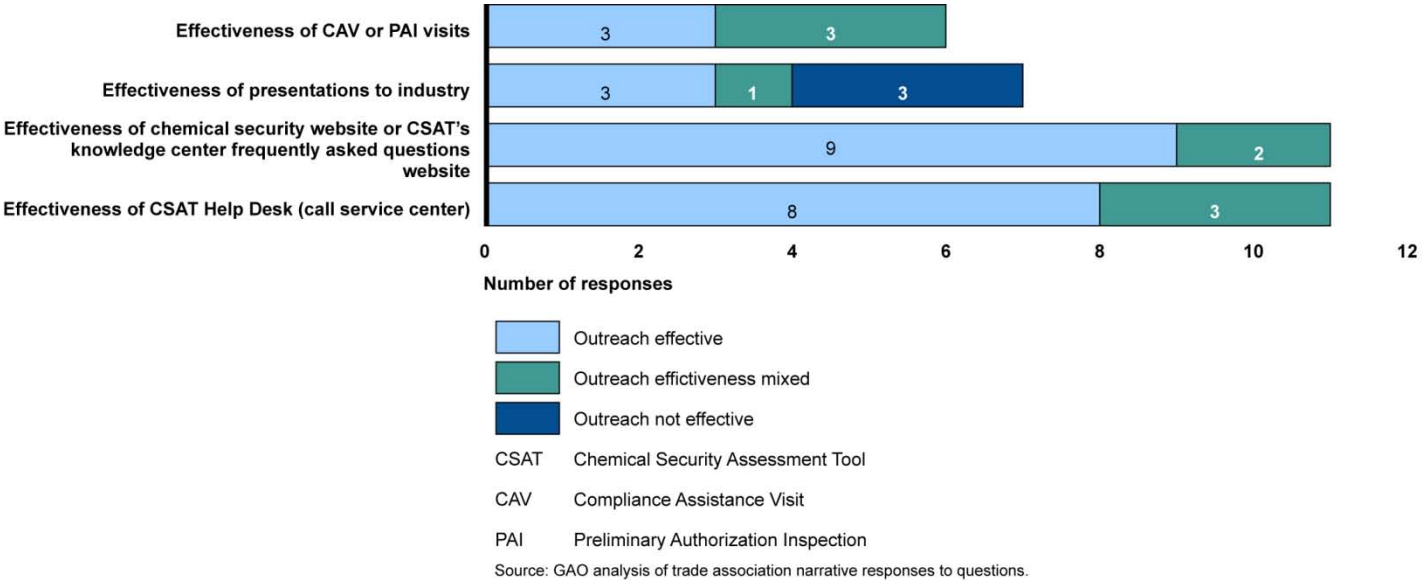
ISCD's tracking system was automated in June 2010—during the early years of the program, outreach reporting was manual. Third, ISCD officials stated that ISCD staffing increases made it possible to perform more outreach to regulated stakeholders. They said that, prior to fiscal year 2009, field staff consisted of about 30 staff detailed from DHS's Federal Protective Service and in subsequent years ISCD increased the size of its field staff to more than 100.

Selected Trade Associations Had Mixed Views about ISCD Efforts to Communicate with Owners and Operators

Our analysis of industry 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 outreach efforts. Whereas 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.[45] Our analysis also showed that trade associations that responded, in general, viewed specific types of ISCD outreach to be either effective or of mixed effectiveness (fig. 4 shows our analysis of trade association responses to questions about specific types of ISCD's outreach activities).

[45]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.

Figure 4: Summary of Trade Association Responses Indicating the Effectiveness of Infrastructure Security Compliance Division (ISCD) Outreach Activities by Type of Outreach

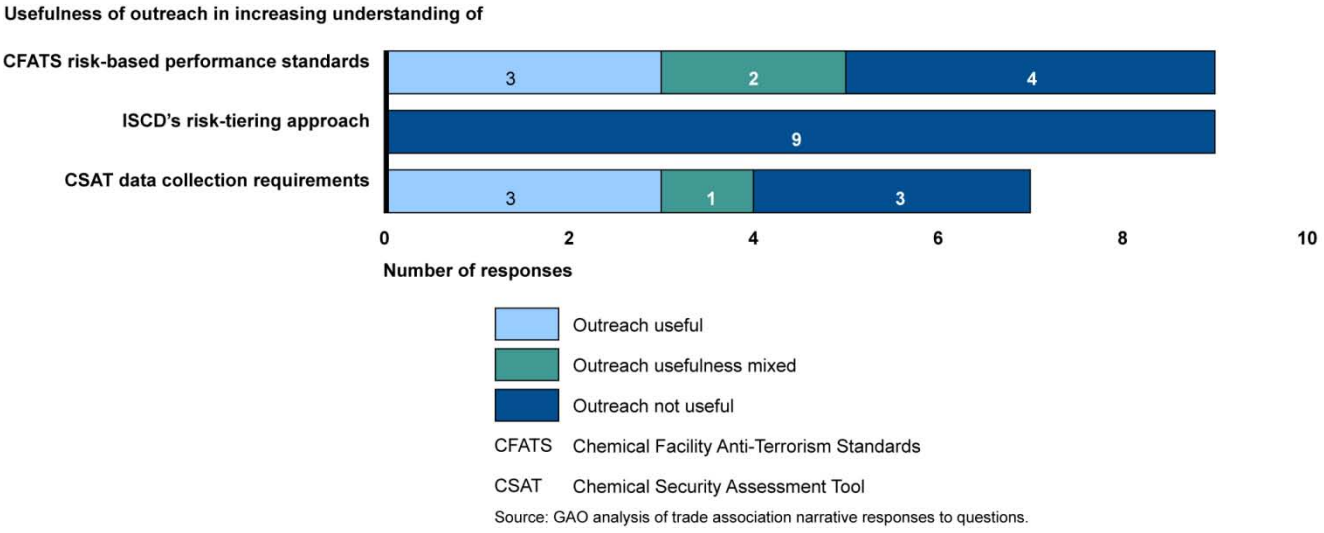


Source: GAO analysis of trade association narrative responses to questions.

Note: Respondents that did not respond (either reported they did not know the answer, did not answer the question, or for whom the question was not applicable) are not represented in the chart.

We also analyzed trade association responses with regard to the usefulness of ISCD outreach activity in terms of their members' understanding of performance standards, tiering approach, and data collection requirements, as shown in figure 5.

Figure 5: Summary of Trade Association Responses on the Usefulness of Outreach Activities in Increasing Understanding of Infrastructure Security Compliance Division (ISCD) Performance Standards, Tiering Approach, and Data Collection Requirements



Source: GAO analysis of trade association narrative responses to questions.

Note: Respondents that did not respond (either reported they did not know the answer, did not answer the question, or for whom the question was not applicable) are not represented in the chart.

Mixed Views on Risk- Based Performance Standards Outreach

Our analysis of trade association responses to our questions showed that opinions were mixed regarding the usefulness of outreach activities related to helping regulated facilities understand the Risk-Based Performance Standards. Specifically, trade association responses showed that 5 of the 11 associations that responded indicated that outreach was useful or had mixed usefulness and 4 associations reported that it was not useful.[46] For example, among those trade associations that indicated that outreach on the performance standards was useful, one reported that outreach activities have helped members better understand the standards and another reported that performance standards guidance and early presentations were also helpful. Conversely, among those that indicated they did not believe outreach on the Risk-Based Performance Standards was useful, one cited a lack of ISCD training on the standards

[46]One respondent said he had not heard feedback from members of his association regarding outreach activities, and another respondent did not answer our question.

and another reported that ISCD needed to provide more assistance to explain what would or would not be compliant using the standards.[47]

Outreach on Facility Risk-Tiering Approach Not Viewed as Useful

Nearly all (9 of 11) trade association respondents indicated that ISCD's outreach to members was not useful in helping them understand the tiering approach used to determine the risk levels of regulated facilities, which they viewed as not being transparent.[48] Three trade association respondents reported that the lack of transparency can hinder facility owners and operators' ability to properly make risk reduction decisions; and 6 respondents reported that there are instances where tiering results contradict the facility's perception of what is "high risk" or conflict with results at similar facilities with similar chemical holdings and population densities in surrounding communities.[49] One member company of 1 trade association reported that industry has repeatedly asked for information on the tiering process without success. ISCD officials told us that they do not currently provide regulated facilities with details about the CFATS risk-tiering approach but noted that one of the tasks of the aforementioned expert panel review is to make recommendations regarding what additional tiering-related information should be provided to facilities. DHS has designated some parts of the risk models as Chemical-terrorism Vulnerability Information—which warrants special treatment for handling and sharing, including assessing whether or not there is a need to know—and other parts of the models as Secret.[50] ISCD officials also stated that they have not received a formal request by facilities asking ISCD to recheck assigned tiering levels or to re-evaluate the output of the risk models because facilities believe the methodology used is faulty.

[47]ISCD officials said that the CFATS statute and regulation specify that they cannot be prescriptive when providing suggestions for increasing security, which they noted has been a challenge. However, officials said that when they have sufficient information (based on facilities that have had their security plans approved), they likely will draft "best practices" that are centered on notional facilities to give industry a point of reference.

[48]One respondent said that he was not well positioned to comment on the usefulness of ISCD's tiering-related outreach activities because of a lack of information from owners and operators the association represented. Another respondent indicated that that the association was not aware that ISCD had conducted outreach in this area.

[49]Some of the specific observations made by trade associations were not necessarily related to particular questions we asked, but rather were common themes mentioned by respondents throughout their responses to our open-ended questions.

[50]Chemical-terrorism Vulnerability Information includes information listed in 6 C.F.R. § 27.400(b).

According to these officials, the primary request from facilities is to know how their facilities were tiered, and industry requests for information mainly come from facilities that either believe they should not be tiered or tiered facilities that are questioning why a neighboring facility has not been tiered.

Mixed Views about Data Collection Outreach

Our query of selected trade associations also showed that they generally had mixed views about ISCD's outreach on data collection requirements. Specifically, 4 of the 11 association officials that provided responses to our query reported that ISCD's outreach efforts had either been useful or had been of mixed usefulness in enabling them to better understand and comply with the ISCD's data collection requirements; 3 reported that outreach on data collection requirements had not been useful; and 4 did not answer the question. Among the 4 respondents that found outreach on data collection requirements to be useful or of mixed usefulness, 1 noted that ISCD had done more outreach specifically on elements of the site security plan, which has broadened stakeholders understanding of the type of information DHS is looking for and options they may not have previously considered. Of the 3 that reported ISCD's outreach on data collection requirements had not been useful, 1 trade association respondent reported that, in 2009, industry representatives had suggested that ISCD produce a document providing tips and suggestions for completing site security plans and reported that it took 3 years for ISCD to produce such a document; similarly, 2 member companies of another trade association reported that ISCD's outreach had not been useful in increasing understanding of data collection requirements, and 1 cited the experience of an individual that seemed confused on much of the information being requested.

Trade Associations We Contacted Expressed Concern about the Burden of Responding to Data Collection Requirements which ISCD Has Plans to Address

Most of the trade associations that responded to our questions also expressed concern about CSAT data collection requirements specifically with regard to various applications such as the Top Screen, vulnerability assessment, and site security plan. Specifically, our analysis of responses by the 11 trade associations indicated that nearly all (9 of 11 respondents) believed that the CSAT data collection effort was burdensome for regulated owners and operators; the other 2 trade associations provided mixed responses. Nine industry trade associations reported that the CSAT data submission requirements take significant resources (such as time and personnel) to prepare, and 10 questioned

the value of the tools in reducing risk or increasing security.[51] One trade association official reported that completing the Top Screen, vulnerability assessment, and security plan data collection effort required over 200 person hours. Another association official reported that the vulnerability assessment data collection requirements were very burdensome and noted that one member's security plan covered 1,400 questions and was nearly 300 pages long.

ISCD officials acknowledged that CSAT can be burdensome and they intend to introduce improvements to CSAT to assist facilities in developing and submitting their Top Screens, security vulnerability assessments, and site security plans. In ISCD's December 2012 *Annual Operating Plan*, one action item calls for the revision of the CSAT based on engagement with industry in order to create a more efficient and effective tool. ISCD officials stated that they estimate that revisions to CSAT will be in place sometime in 2014. According to these officials, improvements being considered for CSAT applications include a reduction in the number of text-based responses and narrative information required in the vulnerability assessment and the site security plan; the inclusion of more drop-down menu options, which is also expected to improve data analysis; and a reduction of the number of repetitive questions, for example, in the site security plan. ISCD officials noted that CSAT can be burdensome when facilities have to reenter data from one document to the next and stated that they are looking to revise CSAT so that information already entered on one document automatically populates data fields covering the same question in the next. ISCD officials also told us that one of the actions ISCD plans to take is to hold three meetings, or roundtable discussions, with industry officials at various locations beginning at the end of February 2013. They said that these discussions are intended to obtain input from industry officials on how CSAT can be improved. ISCD officials said that in making revisions to the CSAT they will consider eliminating unnecessary data requirements, but stated that they may decide to continue to request the data—even if they are not used for risk tiering—because doing so may be helpful to facilities as they prepare their security plans.

[51]Specific observations made by trade associations were not necessarily related to particular questions we asked, but rather were common themes mentioned by respondents throughout their responses to our open-ended questions.

ISCD Does Not Seek Systematic Feedback on the Effectiveness of Its Outreach Efforts

ISCD seeks informal feedback on its outreach efforts but does not systematically solicit feedback to assess the effectiveness of outreach activities,[52] 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 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, gasoline storage site risks, and the personnel surety program. 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 assistance visits to obtain their views on the effectiveness of the outreach.

ISCD, as part of its annual operating plan, has a priority for fiscal year 2013 to develop a strategic communications plan intended to address both internal and external communication needs including industry outreach. One goal in the plan is to maintain robust communication and outreach. In addition, the annual operating plan contains 27 monitoring and performance measures that address outreach program activities, but only one of these calls for ISCD to solicit feedback to assess and measure the effectiveness of the program. The NIPP states that when the government is provided with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly. We have previously reported on the benefits of soliciting systematic feedback. Specifically our prior work on customer service efforts in the government, systematic feedback from regulated facility owners and operators to among other things, determine the kind and quality of services they want and also

[52]ISCD solicits voluntary feedback via a three question survey provided to CSAT Help Desk users on their experience with call center representatives. The survey asks three questions, did service meet expectations, were questions answered in a timely manner and was call service representative (CSR) friendly and knowledgeable.

determine their level of satisfaction with existing services including outreach may benefit to organizations like ISCD that service the public.[53]

As ISCD develops its strategic communication plan, options for gathering feedback on outreach possibly could include using formal surveys reviewed and approved by the Office of Management and Budget (OMB) under the Paperwork Reduction Act;[54] soliciting feedback from regulated owners and operators as a part of after-action reviews conducted at assistance visits, meeting and presentations; working with trade associations or other representatives of the regulated community to design and conduct member surveys; or working with members of various critical infrastructure sectors, such as the chemical or energy sectors, to develop and conduct surveys of sector owners and operators. Given the mixed perspectives of the trade associations we queried, systematic feedback about outreach activities might better position ISCD to identify problems and target changes to its outreach efforts, if necessary, or improve CFATS program outcomes in general. Doing so would also be consistent with Standards for Internal Control in the Federal Government, which call for top level reviews of actual performance and the establishment and review of performance measures and indicators.

Conclusions

ISCD has taken action to assign facilities to risk based tiers, revise its process to review site security plans, and work with facilities to improve security. However, three factors could affect program operations as ISCD moves forward:

- The first factor is a risk assessment approach that is not yet complete because it does not consider all of the elements of risk called for by the NIPP and the CFATS rule. ISCD has begun to take some actions to develop a more robust risk assessment approach, but ISCD would be better positioned to assess risk if it developed an overall plan, with milestones and time frames, incorporating the results of the various efforts to more fully address each of the three components of risk—consequence, threat, and vulnerability—and take actions to enhance the current risk assessment approach. ISCD has commissioned an

[53]GAO, *Managing for Results: Opportunities to Strengthen Agencies' Customer Service Efforts*, GAO-11-44, (Washington, D.C.: October 27, 2010).

[54]44 U.S.C. §§ 3501-3522.

expert panel to identify the strengths and weaknesses of the current risk assessment approach and the results of the panel's work could help ISCD identify issues for further review and recommendations for improvements. This effort and the results from it represent one component of the various efforts ISCD will have to consider moving forward to ensure that the risk assessment approach is complete per the NIPP and the CFATS rule. After ISCD has developed and completed its efforts to enhance its risk assessment approach by using the results of the current expert panel's efforts as well as incorporating the issues we identified along with the Sandia National Laboratories' work on economic consequences, 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 and CFATS rule.

- The second factor is ISCD's ability to measure its progress reviewing site security plans under its revised review process. ISCD has developed measures to assess its progress reviewing site security plans and has recently implemented a plan to measure various aspects of the process. ISCD's efforts appear to be a step in the right direction, but, it will take time for ISCD to collect enough data to develop baselines and begin measuring its performance. While it could take years before ISCD can review and approve the site security plans currently in its queue, ISCD intends to explore ways that it can accelerate the process. Thus, we are not making recommendations at this time.

- The third factor is exploring opportunities to establish a mechanism to systematically gather feedback to measure the effectiveness of ISCD outreach efforts with facility owners and operators. This includes ISCD efforts to communicate with owners and operators on various aspects of the program, such as the development of site security plans, and work with them to better understand how and whether data collection requirements are burdensome and can be reduced. Doing so would be consistent with (1) the NIPP which states that once the government understands private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly, and (2) our past work on the benefits of soliciting feedback to determine customer level of satisfaction with existing services, including outreach. In addition, by obtaining systematic feedback on its outreach efforts, ISCD might be better positioned to (1) identify problems and target program changes, if necessary, and generally improve ISCD efforts to communicate and

work with facility owners and operators, and (2) measure its performance consistent with our Standards for Internal Control in the Federal Government.

Recommendations for Executive Action

To better assess risk associated with facilities that use, process, or store chemicals of interest consistent with the NIPP and the CFATS rule, we recommend the Secretary of Homeland Security direct the Under Secretary for NPPD, the Assistant Secretary for IP, and Director of ISCD to take the following two actions:

- develop a plan, with timeframes and milestones, that incorporates the results of the various efforts to fully address each of the components of risk and take associated actions where appropriate to enhance ISCD's risk assessment approach consistent with the NIPP and the CFATS rule, and
- conduct an independent peer review, after ISCD completes enhancements to its risk assessment approach, that fully validates and verifies ISCD's risk assessment approach consistent with the recommendations of the National Research Council of the National Academies.

To enhance ISCD efforts to communicate and work with facilities, we recommend that the Secretary of Homeland Security direct the Under Secretary for NPPD, the Assistant Secretary for IP, and the Director of ISCD to explore opportunities and take action to systematically solicit and document feedback on facility outreach consistent with ISCD efforts to develop a strategic communication plan.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security for review and comment, which are reprinted in appendix II. In its written comments, DHS agreed with our recommendations and stated that it has efforts underway that will address them. Regarding our first recommendation that ISCD develop a plan, with timeframes and milestones, to fully address each of the components of risk and take associated actions where appropriate to enhance ISCD's risk assessment approach consistent with the NIPP and the CFATS rule, DHS plans to document all processes and procedures related to the risk assessment approach and conduct an internal DHS review of the complete risk assessment process, among others things, to ensure that all elements of risk are included in the risk assessment approach. Regarding our second recommendation that ISCD conduct an independent peer review, after it

completes enhancements to its risk assessment approach, that fully validates and verifies ISCD's risk assessment approach consistent with the recommendations of the National Research Council of the National Academies, DHS agreed that a peer review that includes validation and verification steps would be a worthwhile endeavor, once any changes that result from the aforementioned review of the risk assessment approach are implemented. Regarding our third recommendation that ISCD explore opportunities and take action to systematically solicit and document feedback on facility outreach consistent with ISCD efforts to develop a strategic communication plan, DHS plans to explore such opportunities to make CFATS-related outreach efforts more effective for all stakeholders. DHS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to interested congressional committees and to the Secretary of the Department of Homeland Security. In addition, the report will be available at no charge on GAO's website at http://www.gao.gov. If you or your staff members have any questions about this report, please contact me 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 report. GAO staff who made major contributions to this report are listed in appendix III.

Stephen L. Caldwell
Director
Homeland Security and Justice

List of Congressional Requesters

The Honorable Tom Carper
Chairman
The Honorable Tom Coburn, M.D.
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable John D. Rockefeller IV
Chairman
Committee on Commerce, Science,
and Transportation
United States Senate

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Fred Upton
Chairman
The Honorable Henry A. Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Frank R. Lautenberg
Chairman
Subcommittee on Superfund, Toxics,
and Environmental Health
Committee on Environment and Public Works
United States Senate

The Honorable John P. Carter
Chairman
The Honorable David E. Price
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The Honorable Patrick Meehan
Chairman
The Honorable Yvette D. Clarke
Ranking Member
Subcommittee on Cybersecurity Infrastructure
Protection, and Security Technologies
Committee on Homeland Security
House of Representatives

The Honorable John Shimkus
Chairman
The Honorable Paul Tonko
Ranking Member
Subcommittee on Environment and the Economy
Committee on Energy and Commerce
House of Representatives

The Honorable Susan M. Collins
United States Senate

The Honorable Robert B. Aderholt
House of Representatives

The Honorable Gene Green
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report is a follow-on engagement of work we completed in July 2012 about the actions the Department of Homeland Security's (DHS) Infrastructure Security Compliance Division (ISCD) took related to an internal memorandum that cited an array of challenges—including human capital and administrative issues—that hindered the implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) program.[1] This report discusses the extent to which DHS has

- assigned chemical facilities to risk-based tiers and assessed its approach for doing so,
- revised the process to review security plans, and
- communicated and worked with facilities to help improve security.

To determine the extent to which DHS has assigned chemical facilities to risk-based tiers and assessed its approach for doing so, we reviewed ISCD applications and documents including web-based Chemical Security Assessment Tools (CSAT) applications—such as the Top-Screen and security vulnerability assessment—used to collect security information from facilities, the ISCD risk assessment approach used to determine a facility's risk tier, policies and procedures on tiering, as well as a sample copy of a facility's Top Screen and security vulnerability assessment. In addition, we outlined the risk tiering models associated with different security issues—release, theft or diversion, and sabotage. We also reviewed DHS memoranda detailing the challenges with the release security issue model and ISCD's work to improve it. We compared our review to various criteria including the risk framework outlined in the CFATS statute and rule,[2] the National Infrastructure Protection Plan (NIPP),[3] and risk modeling best practices as outlined by

[1]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).

[2]Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006); 6 C.F.R. pt. § 27.105.

[3]DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). The NIPP sets forth the risk management framework for the protection and resilience of the nation's critical infrastructure. 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). Broadly defined, risk management is a process that helps policymakers assess risk, strategically allocate finite resources, and take actions under conditions of uncertainty.

the National Research Council of the National Academy of Sciences[4] to determine if ISCD's risk assessment approach comports with these criteria and if not, where gaps or deficiencies exist. We also obtained data from ISCD's CSAT system that showed how many of the roughly 3,500 facilities, which ISCD has determined to be regulated by CFATS, were placed in each of the 4 risk-based tiers and what their related security issue(s) was. Because data in the system change regularly, these data represent a snapshot of finally tiered facilities as of January 24, 2013. To assess the reliability of the data we obtained from CSAT, we reviewed system documentation, compared similar datasets for consistency, and interviewed knowledgeable ISCD officials about system controls and determined that the CSAT data were sufficiently reliable for the purposes of this report. We also reviewed documents related to ISCD's ongoing review of the risk assessment approach including the statement of objectives, task execution plan, and terms of reference and compared these documents with the criteria for peer review as laid out by the National Research Council of the National Academy of Sciences as well as past GAO work on peer review.[5] To corroborate and confirm our understanding of the risk assessment approach, we interviewed DHS and contracting officials knowledgeable about the methodology behind the models and their strengths and weaknesses. We also interviewed DHS and contracting officials responsible for the review about the review's scope and progress, and to corroborate and confirm our understanding of the review.

To determine the extent to which DHS has revised its process to review security plans, we reviewed and analyzed documents, where available, including the CFATS statute and rule, the November 2011 internal memorandum, DHS's Risk-Based Performance Standards Guidance, ISCD security plan review policies and procedures, security plan review memoranda, and the instructions used by facilities to prepare and submit security plans. As a part of our review of security plan documents, we

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

[5]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, 2010), *and 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).

identified progress made and challenges encountered by ISCD as the security plan review process evolved. To confirm our understanding of the security plan review process and how it has evolved, we gathered and analyzed statistics pertinent to the process to determine how many site security plans had been reviewed, authorized, and approved as a percent of the total number of security plans submitted. We then used the number of plans approved, along with ISCD officials' estimates of how many plans they intend to approve per month beginning in calendar year 2013 to estimate how long it might take ISCD to review and approve site security plans for the approximately 3,500 currently regulated facilities. We also interviewed ISCD officials about the security plan review process to corroborate the information obtained from ISCD documents and the results of our analyses.

To determine the extent to which DHS has communicated and worked with facilities to help improve security, we reviewed documents (e.g., ISCD's standard operating procedures for conducting compliance assistance visits, inspections, and help desk support). We also reviewed ISCD data on outreach activities—such as the type and number of field visits to facilities and presentations to industry—for fiscal year 2007 through November 30, 2012 that we obtained from CHEMS. As noted above, we determined that data from the CHEMS system were sufficiently reliable for the purposes of this report. In addition, we contacted officials representing 15 trade associations whose members are facilities regulated by CFATS to obtain their perspectives on DHS's efforts to communicate and work with facility owners and operators to help improve security. We selected these 15 trade associations because they are listed in an annex to the NIPP as those with which DHS works on a regular basis on chemical security matters. According to this annex, working with these industry associations is 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. According to the NIPP, a Sector Coordinating Council is the principal entity under which owners and operators of critical infrastructure can coordinate with the government on a wide range of protection activities and issues. The Chemical Sector Coordinating Council represents a significant majority of the owners and operators in the chemical sector. We sent a list of open-ended questions to representatives at each of the 15 trade associations and received responses from 11 trade association representatives. We analyzed, categorized, and summarized these responses by using a systematic content analysis of the open-ended responses to determine the trade association views. As a part of our analysis, two analysts reviewed the responses, developed categories to be used for the content

analysis, and worked together to categorize each open-ended answer. A third analyst reviewed this categorization and verified that the answers were placed in the appropriate categories. Any disagreements regarding the categorization of the answers were subsequently reconciled. The information we obtained from the 11 trade associations that responded is not generalizable to the universe of chemical facilities covered by CFATS; however, it does provide insights into DHS efforts to perform outreach and seek feedback on the implementation of the CFATS rule. We compared the results of our analysis of the responses received from the trade associations and other audit work related to ISCD's outreach efforts to various criteria, including CFATS statute and rule, the NIPP, past GAO work on industry outreach,[6] and internal control standards[7] to determine if DHS's outreach efforts comport with these criteria, and if not, determined where gaps exist. We also interviewed knowledgeable ISCD officials regarding their outreach efforts.

We identified three limitations that should be considered when using our results. First, as noted in our previous work, documentary evidence about the development of the CFATS program is, for the most part, not available. Program officials did not maintain records of key decisions made in the early years of the program and the basis for these decisions. This applies particularly to the risk tiering methodology and the security plan review process. Furthermore, ISCD officials told us many of the individuals involved in these decisions are no longer at ISCD. During discussions, the current management team qualified that much of what they told us about these decisions is their best guess of what happened and why. This limits our ability to fully assess the risk model and compare the original site security plan review process with the process currently in place. Second, with regard to our work with facility owners and operators, we limited our review to industry associations primarily due to time constraints and the large number of owners and operators in the chemical sector. As a result, we could not generalize our findings to the universe of CFATS-regulated facility owners and operators. We mitigated this limitation by contacting 15 industry associations that represented a wide range of CFATS regulated chemical facilities. Third, given that ISCD had

[6]GAO, *Managing for Results: Opportunities to Strengthen Agencies' Customer Service Efforts*, GAO-11-44, (Washington D.C.: Oct. 27, 2010).

[7]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

only recently begun to approve security plans, our scope did not include the facility compliance inspection process (which is based on the results of the approved security plans).

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.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 25, 2013

Mr. Stephen L. Caldwell
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: GAO Draft Report 13-353, "CRITICAL INFRASTRUCTURE PROTECTION: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened"

Dear Mr. Caldwell:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

While recognizing that more can be done to strengthen the Chemical Facility Anti-Terrorism Standards (CFATS) Program, DHS has significantly advanced the program during the past 12 months including:

- Implementing a revised site security plan (SSP) review process, which has increased the pace of SSP reviews;
- Retraining chemical security inspectors on updated inspection protocols, which has allowed for a significant increase in the pace of authorization inspections (AIs); and
- Documenting nine critical processes through standard operating procedures.

As of March 1, 2013, these efforts have enabled the Department to authorize 263 SSPs, conduct 131 AIs, and approve 35 SSPs and three alternative security programs (ASPs) submitted in lieu of the SSP. DHS is on pace to authorize, inspect, and approve between 30 and 50 SSPs per month and is continuing to explore ways to further increase the pace of performance as it moves into Tier 3 and Tier 4 SSP reviews.

This increased SSP review and inspection pace follows the progress made in other CFATS activities since the program's inception. These successes include the processing of more than 43,000 top-screens submitted by chemical facilities, the notification of more than 7,800 facilities of initial high-risk tier determinations, the receipt and review of more than 7,000 security vulnerability assessments, the assignment of nearly 4,000 final tier determinations, and the collection of nearly 4,000 SSPs or ASPs submitted in lieu of SSPs.

During this time, DHS has also been proactively engaged in outreach and communication efforts with the regulated community and other stakeholders. As noted in the report, DHS has conducted thousands of outreach activities, to include more than 1,300 compliance assistance visits and 4,500 outreach engagements to chemical facilities, and nearly 5,000 meetings with federal, state, local, and private industry stakeholders. Finally, since the inception of CFATS, nearly 3,000 facilities have removed, reduced, or otherwise modified their chemical holdings so that they are no longer considered high-risk. All of these activities have helped make our communities more secure.

While DHS has seen many recent successes in implementing CFATS, there remains room for improvement in aspects of the program. Three of these areas are the subject of the report: the manner in which the Department assigns chemical facilities to risk-based tiers, the method the Department uses to review security plans, and the way the Department has communicated and worked with facilities to help improve security. As the report notes, the Department continues to take steps to improve in these areas.

As part of its overall risk management approach, the current CFATS process considers all three traditional risk elements—consequences, vulnerability, and threat—at various junctures throughout the process. However, DHS is also working to identify ways to further improve its tiering methodology, including seeking recommendations from the external peer review and working with Sandia National Laboratories to help the Department add an economic criticality component to its risk tiering methodology. First, as GAO notes, the Department currently considers only health and human-impact consequences and does not assess economic consequences as part of its risk tiering model. Incorporating economic consequences has always been part of the long-term vision for the CFATS model. Second, the Department agrees with GAO's observation that more up-to-date threat information could be used within the tiering methodology, and the Department is committed to regularly updating the threat information. Finally, the Department has contracted to oversee an external peer review of the entire CFATS risk tiering methodology. As part of its efforts, the Department has asked the peer review members to examine some specific concerns GAO raised that DHS previously identified as potential areas for improvement, to include how threat is applied to theft-and-diversion chemicals of interest and how vulnerability is considered throughout the risk model. All of these efforts demonstrate the Department's commitment to enhancing the CFATS overall risk methodology.

DHS has also made great strides in the second area reviewed by GAO—the method the Department uses to review security plans—and continues to seek ways to improve this critical element of the CFATS program. Within the past 12 months the Department has modified its SSP review and inspection processes, which has turned the previous trickle of SSP authorizations and facility inspections into a steady stream of approvals of SSPs and ASPs. As noted above and within the report, the updated SSP review and inspection processes have helped the Department progress to being able to authorize, inspect, and approve between 30 and 50 security plans per month. Nevertheless, DHS is continuing to address the backlog and explore ways to make the process even more efficient and effective as we move into reviews and inspections at Tier 3 and Tier 4 facilities. Options currently being explored include the increased use of ASPs and a review of the current processes to identify further opportunities for streamlining.

The Department appreciates GAO's recognition of our efforts regarding communication with and outreach to members of the regulated community and other stakeholders. Although DHS has received primarily positive feedback on our outreach and communications efforts from the regulated community, we acknowledge there is room for improvement. For example, recognizing that regulated facilities best understand their risk drivers and in support of increased transparency, the Department is analyzing which aspects of the risk methodology it can and should share with members of the regulated community. Similarly, the Department is aware of the regulated community's concern with the significant burden the CFATS data collection processes can impose on more complex facilities. To address this concern and other needed information technology (IT) improvements, the Department is undertaking an effort to modify its IT systems to make them more user friendly for the regulated community. As part of this effort, the Department is holding a series of roundtables with members of the regulated community to solicit input on how to make the tools less burdensome and more useful.

The draft report contained three recommendations, with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the Under Secretary for the National Protection and Programs Directorate, the Assistant Secretary for the Office of Infrastructure Protection, and the Director of the Infrastructure Security Compliance Division (ISCD) to:

Recommendation 1: Develop a plan with time frames and milestones that incorporate the results of the various efforts to fully address each component of risk, and to take associated actions, where appropriate, to enhance ISCD's risk assessment approach consistent with the National Infrastructure Protection Plan and the CFATS rule.

Response: Concur. As discussed above and as GAO noted in its report, the Department is taking a number of steps to review its current risk methodology and ensure that all three traditional security risk factors (i.e., consequences, vulnerability, and threat) are appropriately considered in the overall CFATS risk-based process. These steps include documenting all processes and procedures related to the tiering methodology, conducting an internal DHS review of the complete tiering process, conducting an external peer review of the risk-based tiering methodology, and engaging Sandia National Laboratories to assist the Department in developing a model for identifying and tiering high-risk chemical facilities on the basis of economic consequences. The Department will use the results of these efforts to improve the CFATS tiering model, as appropriate, by developing an integrated plan with time frames and milestones. Following implementation of any changes, a second peer review, including formal verification and validation, may be appropriate. It is worth noting, however, there are varying approaches for prioritizing at-risk infrastructure, as mentioned in other GAO work products. Estimated Completion Date (ECD): To Be Determined (TBD).

Recommendation 2: Conduct an independent peer review after ISCD completes enhancements to its risk assessment approach that fully validate and verify ISCD's risk management approach consistent with the recommendations of the National Research Council of the National Academies.

3

Response: Concur. Although the Department believes that the current external peer review will accomplish much of what GAO is recommending, the Department agrees that a second peer review is a worthwhile endeavor, following implementation of any changes based on the activities covered by Recommendation 1, including formal verification and validation. ECD: TBD

Recommendation 3: Explore opportunities and take action to systematically solicit and document feedback on facility outreach consistent with ISCD efforts to develop a strategic communication plan.

Response: Concur. More efforts to systematically solicit and document feedback on CFATS-related outreach activities will enable the Department to identify those outreach efforts having the greatest impact and to make improvements across the board on all outreach and engagement efforts. The Department is committed to exploring different opportunities to solicit and document feedback on outreach activities for the purpose of making CFATS-related outreach efforts more effective for all stakeholders. ECD: TBD

Again, thank you for the opportunity to review and provide comments on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in future.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

4

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen L. Caldwell, (202) 512-8777 or CaldwellS@gao.gov

Staff Acknowledgments

In addition to the contact named above, John F. Mortin, Assistant Director, and Ellen Wolfe, Analyst-in-Charge; Chuck Bausell; Jose Cardenas; Michele Fejfar; Jeff Jensen; Tracey King; Marvin McGill; made significant contributions to the work.

Related GAO Products

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: Summary of DHS Actions to Better Manage Its Chemical Security Program. GAO-12-1044T. Washington, D.C.: September 20, 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.