

**GAO**

Testimony

Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

---

For Release on Delivery  
Expected at 10:00 a.m. EDT  
Thursday, July 26, 2012

**CRITICAL  
INFRASTRUCTURE  
PROTECTION**

**DHS Is Taking Action to  
Better Manage Its Chemical  
Security Program, but It Is  
Too Early to Assess Results**

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



**G A O**

Accountability \* Integrity \* Reliability

---

Highlights of [GAO-12-515T](#) a testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives

## Why GAO Did This Study

The events of September 11, 2001, triggered a national re-examination of the security of facilities that use or store hazardous chemicals in quantities that, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death. 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, a component of IP, manages the program. A November 2011 internal ISCD memorandum, prepared by ISCD senior managers, has raised concerns about the management of the program. This testimony focuses on (1) how the memorandum was developed and any challenges identified, (2) what actions are being taken in response to any challenges identified, and (3) the extent to which ISCD's proposed solutions require collaboration with NPPD or IP. GAO's comments are based on recently completed work analyzing the memorandum and related actions. GAO reviewed laws, regulations, DHS's internal memorandum and action plans, and related documents, and interviewed DHS officials.

## What GAO Recommends

GAO recommends that DHS look for opportunities, where practical, to measure its performance implementing actions items. DHS concurred with the recommendation.

View [GAO-12-515T](#). For more information, contact Stephen L. Caldwell, (202) 512-8777, [CaldwellS@gao.gov](mailto:CaldwellS@gao.gov).

July 2012

## CRITICAL INFRASTRUCTURE PROTECTION

### DHS Is Taking Action to Better Manage Its Chemical Security Program, But It Is Too Early to Assess Results

## What GAO Found

The November 2011 memorandum that discussed the management of the Chemical Facility Anti-Terrorism Standards (CFATS) program was prepared based primarily on the observations of the Director of the Department of Homeland Security's (DHS) Infrastructure Compliance Security Division (ISCD), a component of the Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD). The memorandum was intended to highlight various challenges that have hindered ISCD efforts to implement the CFATS program. According to the Director, the challenges facing ISCD included not having a fully developed direction and plan for implementing the program, hiring staff without establishing need, and inconsistent ISCD leadership—factors that the Director believed place the CFATS program at risk. These challenges centered on human capital issues, including problems hiring, training, and managing ISCD staff; mission issues, including overcoming problems reviewing facility plans to mitigate security vulnerabilities and performing compliance inspections; and administrative issues, including concerns about NPPD and IP not supporting ISCD's management and administrative functions.

ISCD has begun to take various actions intended to address the human capital management, mission, and administrative issues identified in the ISCD memorandum and has developed a 94-item action plan to track its progress. According to ISCD managers, the plan appears to be a catalyst for addressing some of the long-standing issues the memorandum identified. As of June 2012, ISCD reported that 40 percent (38 of 94) of the items in the plan had been completed. These include (1) requiring ISCD managers to meet with staff to involve them in addressing challenges, clarifying priorities, and changing ISCD's culture and (2) developing a proposal to establish a quality control function over compliance activities. The remaining 60 percent (56 of 94) that were in progress include those requiring longer-term efforts—i.e., streamlining the process for reviewing facility security plans and developing facility inspection processes; those requiring completion of other items in the plan; or those awaiting action by others, such as approvals by ISCD leadership. ISCD appears to be heading in the right direction, but it is too early to tell if individual items are having their desired effect because ISCD is in the early stages of implementing corrective actions and has not established performance measures to assess results. Moving forward, exploring opportunities to develop measures, where practical, to determine where actual performance deviates from expected results, consistent with internal control standards could help ISCD better identify any gaps between actual and expected results so that it can take further action, where needed. For example, as ISCD develops a new security plan review process, it could look for ways to measure the extent to which the time to do these reviews has been reduced as compared with the time needed under the current review process.

According to ISCD officials, almost half of the action items included in the June 2012 action plan require ISCD collaboration with or action by NPPD and IP. The ISCD memorandum stated that IP and NPPD did not provide the support needed to manage the CFATS program when the program was first under development. ISCD, IP, and NPPD officials confirmed that IP and NPPD are providing needed support and stated that the action plan prompted them to work together to address the various human capital and administrative issues identified.

---

Chairman Aderholt, Ranking Member Price, and Members of the Subcommittee:

I am pleased to be here today to discuss the Department of Homeland Security's (DHS) efforts to address various challenges in implementing and managing the Chemical Facility Anti-Terrorism Standards (CFATS) program. The events of September 11, 2001, triggered a national re-examination of the security of facilities that use or store hazardous chemicals in quantities that, in the event of a terrorist attack, could put large numbers of Americans at risk of serious injury or death. Chemicals held at these facilities can be used to cause harm to surrounding populations during terrorist attacks, can be stolen and used as chemical weapons or as precursors (the ingredients for making chemical weapons), or stolen and used to build an improvised explosive device. To mitigate this risk, the DHS appropriations act for fiscal year 2007<sup>1</sup> required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities.<sup>2</sup> DHS established the CFATS program to assess the risk, if any, posed by chemical facilities; place high-risk facilities in one of four risk-based tiers; require high-risk facilities to develop security plans; review these plans; and inspect the facilities to ensure compliance with the regulatory requirements. DHS's National Protection and Programs Directorate (NPPD) is responsible for the CFATS program. Within NPPD, the Infrastructure Security Compliance Division (ISCD), a component of the Office of Infrastructure Protection (IP), manages the program.

A November 2011 internal ISCD memorandum, prepared by ISCD's Director in consultation with the Deputy Director, has raised concerns about the management of the CFATS program. The ISCD memorandum, which was leaked to the media in December 2011, cited an array of challenges that, according to these officials, hindered ISCD's ability to implement and manage the CFATS program.<sup>3</sup> My statement today discusses

---

<sup>1</sup>Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

<sup>2</sup>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.

<sup>3</sup>According to DHS officials, the ISCD memorandum was never intended to be publically released.

- 
- how the memorandum was developed and what challenges were identified;
  - what actions are being taken to address the challenges identified; and
  - the extent to which ISCD's planned actions and proposed solutions require action to be taken by or in collaboration with NPPD or IP.

This statement today is based on work we recently completed for you on this ISCD memorandum and related actions. To conduct this work, we reviewed applicable laws and regulations, as well as NPPD, IP, and ISCD policies and procedures for administering the CFATS program. We also analyzed the ISCD memorandum prepared by the ISCD Director in consultation with the Deputy Director, compared it with the proposed action plan ISCD officials prepared to address the challenges identified, and compared subsequent action plans to monitor ISCD's progress.<sup>4</sup> We interviewed senior ISCD officials (including the ISCD Director and Deputy Director) to discuss the challenges identified and planned corrective actions. We also interviewed NPPD and IP officials to obtain their views on the causes for the challenges, ISCD's proposed actions, and their roles in working with ISCD to address the challenges. We obtained and reviewed available documentation (e.g., standard operating procedures and ISCD memos) relevant to each action item. Finally, we compared the results of our analysis of the proposed action plan, and our discussions with DHS, NPPD, IP, and ISCD officials, with various criteria, including the CFATS law and regulations; DHS policies, procedures and reports; *Standards for Internal Control in the Federal Government*;<sup>5</sup> *The Standard*

---

<sup>4</sup>We initially reviewed an ISCD action plan developed in January 2012. ISCD periodically updated the plan to monitor progress on the action items and we reviewed eight versions of the action plan up to and including one developed in June 2012.

<sup>5</sup>GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD 00-21.3.1 (Washington, D.C.: November 1999). Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing and reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

---

for *Program Management*,<sup>6</sup> and past GAO and DHS Office of Inspector General (OIG) reports.<sup>7</sup> We identified limitations that should be considered when using our results. For example, the ISCD memorandum represented the views of the senior ISCD officials that prepared the memorandum and may not be representative of the views of other officials within the CFATS program. Also, our results are based on ISCD's action plan as of June 2012 so these results reflect the status of ISCD's progress up to that point in time.

We conducted this performance audit from February 2012 to July 2012 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 analysis based on our audit objectives. Appendix I discusses our scope and methodology and related limitations in greater detail.

---

## 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 DHS to issue regulations establishing risk-based performance standards<sup>8</sup> for security of facilities that the Secretary determines to present high levels of security risk.<sup>9</sup> The CFATS rule was published in April 2007<sup>10</sup> and

---

<sup>6</sup>Project Management Institute, *The Standard for Program Management*© (Newtown Square, Pa: 2006). *The Standard for Program Management* provides guidelines for successfully managing programs and projects.

<sup>7</sup>GAO, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, [GAO-03-439](#) (Washington, D.C.: March 2003; DHS OIG, *Use of DHS Purchase Cards*, OIG-11-101 (Washington D.C.: August 2011; and DHS OIG, *The Preparedness Directorate's Anti-Deficiency Act Violations for Fiscal Year 2006 Shared Service Administrative Assessment*; OIG-12-21 (Washington D.C.: December 2011).

<sup>8</sup>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.

<sup>9</sup>Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

---

Appendix A to the rule, published in November 2007, listed 322 chemicals of interest and the screening threshold quantities amount for each.<sup>11</sup> According to the CFATS rule, any facility that possesses (or later comes into possession of) any of these chemicals in quantities that meet or exceed the threshold is required to submit certain information to DHS for screening. According to the rule, if DHS preliminarily determines that a facility is high risk—that is, the facility presents a high risk of significant adverse consequences for human life or health, national security, or critical economic assets if subjected to terrorist attack, compromise, infiltration, or exploitation—the facility must submit a security vulnerability assessment to DHS that identifies security vulnerabilities at the site, among other things. After reviewing the security vulnerability assessment, DHS then makes a final decision as to whether the facility is high-risk and, if so, assigns the facility to a final tier.<sup>12</sup> The rule then requires facilities that have been finally determined to be high-risk to develop and submit for DHS approval site security plans that generally show how they are to address the vulnerabilities identified in the vulnerability assessment, including measures that satisfy applicable risk-based performance standards. In addition, the rule requires that DHS implement a compliance inspection process to ensure that covered facilities are satisfying DHS’s performance standards consistent with their approved site security plans.

ISCD has direct responsibility for implementing DHS’s CFATS rule, including assessing potential risks and identifying high-risk chemical facilities, promoting effective security planning, and ensuring that final high-risk facilities meet the applicable risk-based performance standards through site security plans approved by DHS. ISCD is managed by a Director and a Deputy Director and operates five branches that are, among other things, responsible for information technology operations,

---

<sup>10</sup>72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified at 6 C.F.R. pt. 27).

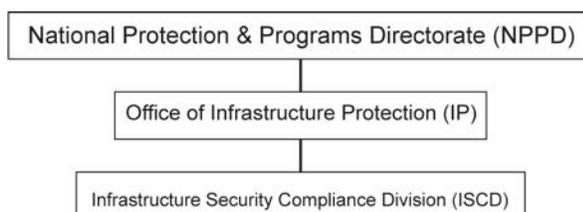
<sup>11</sup>72 Fed. Reg. 65,396 (Nov. 20, 2007). According to DHS, CFATS not only covers facilities that manufacture chemicals but also covers facilities that store or use certain chemicals as part of their daily operations. This can include food-manufacturing facilities that use chemicals of interest in the manufacturing process, farms that use certain quantities of ammonium nitrate or urea fertilizers, or universities that use chemicals to do experiments.

<sup>12</sup>According to DHS officials, tiering determinations are dynamic; for example, a tiering determination can change when a company voluntarily alters its facilities in a way that reduces its risk profile. These officials stated that “final tiering” refers to a tiering assignment following a security vulnerability assessment—it does not imply that this is the final tiering assignment a facility may ever receive.

---

policy and planning; providing compliance and technical support; inspecting facilities and enforcing CFATS regulatory standards; and managing logistics, administration, and chemical security training. ISCD receives business support from NPPD and IP for services related to human capital management and training, budget and finance, and acquisitions and procurement. Figure 1 shows ISCD's current organizational structure within NPPD and IP. Appendix II provides a more detailed organization chart showing the various ISCD divisions.

**Figure 1: NPPD, IP, and ISCD Organizational Structure**



Source: GAO analysis of NPPD, IP, and ISCD organizational charts.

From fiscal years 2007 through 2012, DHS dedicated about \$442 million to the CFATS program. During fiscal year 2012, ISCD was authorized 242 full-time-equivalent positions. For fiscal year 2013, DHS's budget request for the CFATS program was \$75 million and 242 positions.

---

## The CFATS Rule

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 the rule is required to complete an initial screening tool (referred to by DHS as the Top Screen) whereby the facility provides DHS various data, including the name and location of the facility and the chemicals and their quantities at the site.<sup>13</sup> DHS is to use this information to initially determine whether the facility is high risk. 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.

---

<sup>13</sup>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, hydrogen cyanide, 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.

---

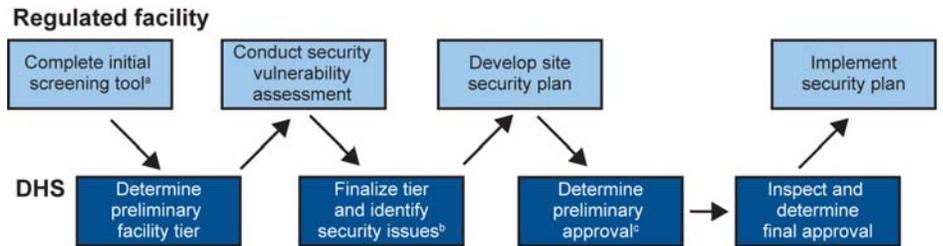
Facilities preliminarily placed in any one of these tiers are considered to be high risk, with tier 1 facilities considered to be the highest risk. Facilities that DHS initially determines to be high risk are required to complete a security vulnerability assessment, which includes the identification of potential critical assets at the facility and a related vulnerability analysis.<sup>14</sup> DHS is to then review the security vulnerability assessment and notify the facility of DHS's final determination as to whether or not it 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. Once this occurs, the facility is required to submit a site security plan or participate in an alternative security program in lieu of a site security plan.<sup>15</sup> 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 will address the applicable risk-based performance standards. DHS then is to do a preliminary review of the security plan to determine whether it meets the regulatory requirements. If these requirements appear to be satisfied, DHS issues a letter of authorization for the facility's plan. DHS then conducts an authorization inspection of the facility and subsequently determines whether to approve the security plan. If DHS determines that the plan does not satisfy CFATS requirements (based on its preliminary review after an authorization inspection), DHS then notifies the facility of any deficiencies and the facility must submit a revised plan correcting those deficiencies. If the facility fails to correct the deficiencies, DHS may then disapprove the plan. Following approval, DHS may conduct further inspections to determine if the facility is in compliance with its approved security plan. Figure 2 illustrates the CFATS regulatory process.

---

<sup>14</sup>Preliminary tier 4 facilities also have the option of submitting an alternate security plan in lieu of a security vulnerability assessment.

<sup>15</sup>Under the CFATS rule, an alternative security program is defined as a third-party or industry organization program; a local authority, state, or federal government program; or any element or aspect thereof that the Assistant Secretary for Infrastructure Protection has determined meets the requirements of the rule and provides for an equivalent level of security to that established by the rule.

**Figure 2: DHS Chemical Facility Anti-Terrorism Standards (CFATS) Regulatory Process**



Source: GAO analysis of DHS CFATS regulatory process.

<sup>a</sup>Facilities are to submit an initial screening tool that provides basic information about the facility and the chemicals they possess.

<sup>b</sup>This step includes determining if a facility is high- risk, and if so, DHS assigns a tier and identifies security issues.

<sup>c</sup>At this stage, if requirements are satisfied, DHS issues a letter of authorization for the facility's plan.

In July 2007, DHS began reviewing information submitted by approximately 40,000 facilities. By January 2012, DHS had preliminarily determined that approximately 4,500 of these facilities were high risk and preliminarily placed each in one of the four tiers. Each of these approximately 4,500 facilities was to complete a security vulnerability assessment, and those facilities that DHS finally determined to be high risk were to submit a site security plan. According to ISCD officials, the vulnerability assessment process prompted over 1,600 facilities to remove chemicals of interest from their sites, thereby enhancing their security posture and removing them from CFATS coverage. Also, according to division officials, as of February 2012, ISCD had worked with facilities to complete 925 compliance assistance visits whereby division inspectors visit high-risk facilities to provide knowledge of and assistance in complying with CFATS, particularly facilities that were in the process of preparing their security plans.

---

## Senior ISCD Leaders Developed the ISCD Memorandum to Highlight Various Challenges Hindering CFATS Implementation

---

### ISCD's Memorandum Based Largely on Observations of Senior ISCD Managers

Our review of the ISCD memorandum and discussions with ISCD officials showed that the memorandum was developed during the latter part of 2011 and was developed primarily based on discussions with ISCD staff and the observations of the ISCD Director in consultation with the Deputy Director. In July 2011, a new Director and Deputy Director were appointed to lead ISCD and, at the direction of NPPD's Under Secretary, began a review of the CFATS program goals, challenges, and potential corrective actions.<sup>16</sup> In November 2011, the Director and Deputy Director provided the Under Secretary the ISCD memorandum entitled "Challenges Facing ISCD, and the Path Forward." These officials stated that the memorandum was developed to inform leadership about the status of ISCD, the challenges it was facing, and the proposed solutions identified to date. In transmitting a copy of the memorandum to congressional stakeholders following the leak in December 2011, the NPPD Under Secretary discussed caveats about the memorandum. He stated that the memorandum was not a formal compliance audit or program review and in several instances it lacked useful, clarifying context. He stated that the ISCD memorandum was not intended for wider internal or external dissemination beyond the Under Secretary's

---

<sup>16</sup>Also prior to July 2011, a former Acting ISCD Director established a working group to address problems related to the original risk assessment computer model problems. The working group was established because ISCD had determined that that some high-risk chemical facilities had been incorrectly categorized. According to the ISCD memorandum, the incorrect categorization called into question the credibility of the program. ISCD determined that about 500 facilities were potentially affected by a data error in the original model, which resulted in changes to many of those facilities' final tier levels or other changes to their final tier results, including some facilities no longer being considered high-risk.

---

office. He further explained that it had not undergone the normal review process by DHS's Executive Secretariat and contained opinions and conclusions that did not reflect the position of DHS. He also noted that the memorandum did not discuss the "significant progress" ISCD had made to date reaching out to facilities of concern to improve their security posture. For example, senior division officials told us that the memorandum did not note the positive impact of ISCD's initial screening of facilities, which resulted in many facilities reducing their holdings of regulated materials so that they would no longer be subject to the rule.

The ISCD Director confirmed that she was the primary author of the ISCD memorandum, in consultation with the Deputy Director, and said that the memorandum was intended to be used as an internal management tool. The Director stated that when she was brought onboard, the Under Secretary tasked her to look at CFATS from an outsider's perspective and identify her thoughts on the program relative to other regulatory regimes, particularly in light of growing concerns about possible human capital issues and problems tiering chemical facilities covered by CFATS. She confirmed that the memo was intended to begin a dialog about the program and challenges it faced. The Director also confirmed that she developed the memorandum by (1) surveying division staff to obtain their opinions on program strengths, challenges, and recommendations for improvement; (2) observing CFATS program operations including the security plan review process; and (3) analyzing an internal DHS report on CFATS operations,<sup>17</sup> which, according to the Director, served as a basis for identifying some administrative challenges and corrective action. The Director told us that senior ISCD officials, including branch chiefs, were given an opportunity to review an initial draft of the memorandum and provided feedback on the assumptions presented. ISCD branch chiefs—the officials responsible for taking corrective actions—confirmed that they were given the opportunity to provide comments on a draft of the memorandum. However, they said that after the leak, almost all of the senior ISCD officials, including branch chiefs, did not have access to the final memorandum per the instruction of the Under Secretary for Management. The senior ISCD and NPPD officials we contacted said that they generally agreed with the material that they saw, but noted that they believed the memorandum was missing context and balance. For

---

<sup>17</sup>DHS Office of Compliance and Security, National Protection and Programs Directorate, *Infrastructure Security Compliance Division (ISCD) Program Inspection*, April-September, 2011.

---

example, one NPPD official stated that that the tone of the memorandum was too negative and the problems it discussed were not supported by sound evaluation. The official expressed the view that the CFATS program is now on the right track.

---

### ISCD Director Was Concerned That Challenges Place the CFATS Program at Risk

The ISCD memorandum discussed numerous challenges that, according to the Director, pose a risk to the program. The Director pointed out that, among other things, ISCD had not approved any site security plans or carried out any compliance inspections on regulated facilities. The Director attributed this to various management challenges, including a lack of planning, poor internal controls, and a workforce whose skills were inadequate to fulfill the program's mission and highlighted several challenges that have an impact on the progress of the program. In addition, the memorandum provided a detailed discussion of the issues or problems facing ISCD. One group of issues focused on human capital management, problems the author categorized as team issues. According to the Director, these included issues arising out of poor staffing decisions; difficulty establishing a team culture that promotes professionalism, respect, and openness; a lack of measurable employee performance goals and unclear performance and conduct standards; and potential delays associated with notifying ISCD inspector union over policies, procedures, and processes. A second group focused on mission issues, including what the author found to be the slow pace of the site security plan approval process, the lack of an established inspection process, and the ISCD's inability to perform compliance inspections 5 1/2 years after enactment of the CFATS statute, and the lack of an established records management system to document key decisions. A third group focused on administrative issues, particularly those the Director regarded as a lack of infrastructure and support, both within ISCD and on the part of NPPD and IP. They included the aforementioned concern about over-reliance on contractors, insufficient and inconsistent support by NPPD and IP with regard to human capital needs—including support on the aforementioned staffing issues—and insufficient controls regarding the use of inspector vehicles, purchase cards, and travel.

Additional details on the human capital, mission, and administrative issues identified in the ISCD memorandum are considered "for official use only."

---

## ISCD Has Begun to Take Various Actions Intended to Address Challenges Identified

---

### ISCD's Action Plan Includes Time Frames for Completing Action Items and Appears to Be a Catalyst for Addressing Some Legacy Issues

ISCD is using an action plan to track its progress addressing the challenges identified in the memorandum, and, according to senior division officials, the plan may be helping them address some legacy issues that staff were attempting to deal with before the memorandum was developed. As discussed earlier, the ISCD memorandum was accompanied by a proposed action plan that, according to the director, was intended to provide proposed solutions to the challenges identified. The January 2012 version of that plan listed 91 actions to be taken categorized by issue—human capital management issues, mission issues, or administrative issues—that, according to the ISCD Director, were developed to be consistent with the ISCD memorandum. Each action item also listed the coordinator, or individual or unit responsible for the action, and discussed the status of the action, including whether the item was complete or in progress. For example, in the human capital/staffing issues area, one action item was intended to engage ISCD leadership to develop an integration plan for newly hired employees. The IP Business Support Team, which is co-located with ISCD, was responsible for coordinating this action, and at the time the plan was prepared, the action was in progress. According to the plan, a 3-day ISCD 101 course had been developed and a more comprehensive process for acclimating new employees to ISCD was under development. However, the January 2012, version of the action plan did not provide information on when the action was started or to be finished.

In February 2012, ISCD developed a version of the action plan that included the same information as the January 2012, plan. However, it also included quarterly projected completion dates. Since then the division's action plan has evolved into a more detailed plan containing 94 items. Like the February 2012 plan, March and June 2012 updated versions of the plan contained information on the coordinator, the action to be taken, and the status of each item. However, unlike the February 2012 version of the plan, the March and June versions of the plan provided detailed milestones and timelines for completing action items including calendar dates, and interim actions leading to completion—

---

essentially a road map for managing each action item according to particular dates and milestones.<sup>18</sup> This approach is consistent with *The Standard for Program Management*, which calls for organizations to develop plans with milestones and time frames to successfully manage programs and projects.<sup>19</sup>

Eleven of the 12 ISCD managers (those other than the Director and Deputy Director) assigned to work as the coordinators of the individual action items told us that even though they were not given the opportunity to view the final version of the ISCD memorandum, the Director provided them the sections of the action plan for which they were responsible to help them develop and implement any corrective actions. They said that they agreed that actions being taken in the plan were needed to resolve challenges facing ISCD. Our discussions with these officials also showed that about 39 percent (37 of 94) of the items in the March and June 2012 action plans addressed some legacy issues that were previously identified and, according to these officials, corrective actions were already under way for all 38 of these action items. For example, one action item called for ISCD to maintain better relations with industry, Congress, and other key stakeholders. ISCD officials said that the ISCD Policy Branch had already begun working on this strategy prior to the development of the memorandum and action plan and that this strategy was given more attention and a higher priority because of the associated action item. An ISCD official expressed the view that the ISCD memorandum and action plan encouraged ISCD to address these and other items sooner than they otherwise might have been addressed.

---

### ISCD's June 2012 Plan Update Showed 38 Action Items Completed

Our analysis of the June 2012 version of the ISCD action plan showed that 40 percent of the items in the plan (38 of 94) had been completed. The remaining 60 percent (56 of 94) were in progress. Our analysis of the 38 completed items showed that 32 of the 38 items were associated with human capital management and administrative issues, including those

---

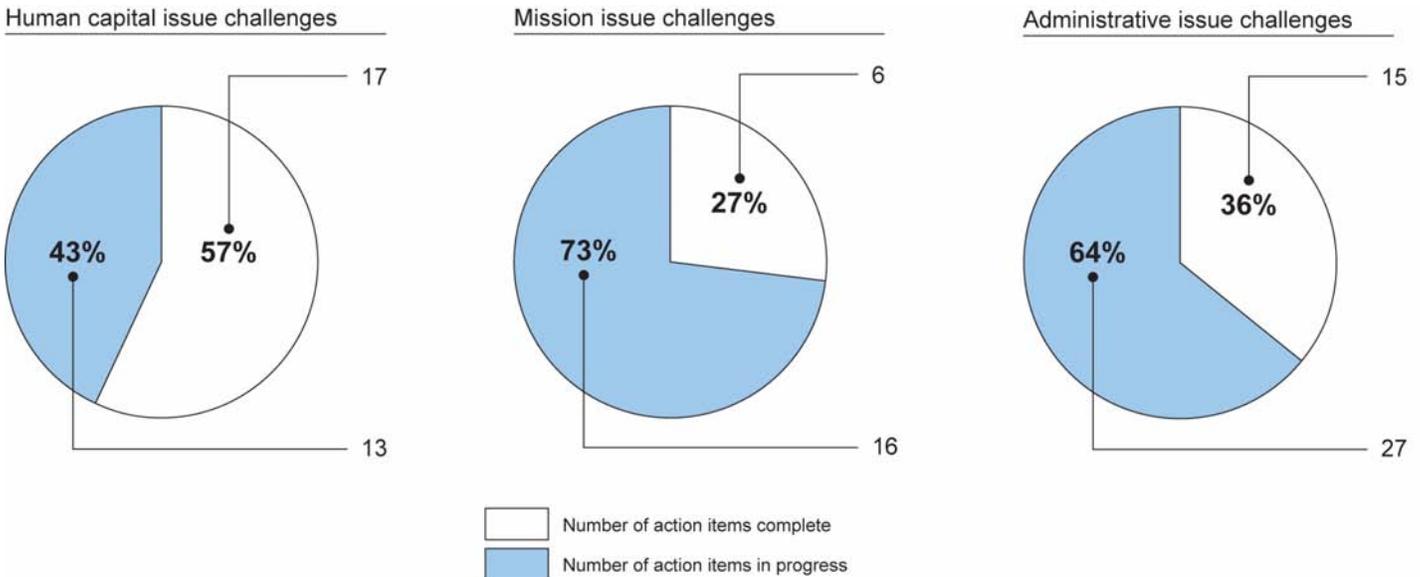
<sup>18</sup>ISCD updated this version of the plan, which is intended to be for official use only, in April 2012 and submitted it to Members of Congress for informational purposes and updated this version again in June 2012. However, the version of the plan submitted to Members of Congress did not contain detailed time frames and milestones; rather it showed timeframes by quarters much like the February version of the plan. Our analysis focused on the detailed version of the plan to help us better assess ISCD's progress.

<sup>19</sup>Project Management Institute, *The Standard for Program Management*.

---

involving culture and human resources, contracting, and documentation. For example, one human capital management issue that is complete called for ISCD to survey staff to obtain their opinions on program strengths and challenges and recommendations for program improvements. According to the June 2012 action plan, the survey was completed and ISCD's action plan showed the item as completed on January 10, 2012. Another completed human capital action item—categorized by ISCD as a cultural issue—called for ISCD management to hold a series of meetings with employees to involve them in addressing program challenges, clarify program priorities related to its mission, and implement changes in ISCD culture. The June 2012 version of the action plan shows the item as completed on January 10, 2012, but noted that this activity will continue going forward. The remaining 6 of 38 action items categorized by ISCD as completed were associated with mission issues such as 1 action item calling for ISCD to establish a quality control function for compliance and enforcement activities. According to ISCD's action plan, this item was completed in April 2012, based on development of a proposal to form the quality control section within the division. Figure 3 shows the status of action items by each of the three categories—human capital management issues, mission issues, and administrative issues, as of June 2012. Appendix III provides an overview of the items in the action plan and their status (completed or in progress) by issue (human capital management, mission issues, and administrative issues) and subcategory.

**Figure 3: Status of ISCD Action Plan by Issue, as of June 2012**



Source: GAO analysis of ISCD data.

For the remaining 56 items that were in progress, 40 involved human capital management and administrative issues. According to ISCD officials, these 40 issues generally involved longer-term efforts—such as organizational realignment—or those that require approval or additional action on the part of IP or NPPD. For example, ISCD reported that there are 13 action items that are directly or indirectly associated with the division’s realignment efforts, including items that require approval by NPPD and IP. The overall realignment effort related to these action items is intended to address concerns, highlighted in the memorandum, that ISCD’s organizational structure was “stovepiped” and compartmentalized. The plan, which, as of June 2012, was in draft, would, according to officials, reorganize ISCD to “integrate more fully certain functions to enhance the collaborative nature of the work that needs to be performed” and would entail creating new offices, moving and integrating others, and centralizing some functions that are now dispersed throughout the division. In accordance with the affected action items, ISCD and a contractor developed the several elements of the realignment plan for review, and ISCD was awaiting input or guidance from NPPD and IP before associated action items can be completed.

Sixteen of 56 remaining actions items in progress covered mission issues that will likely also require long-term efforts to address. For example, 1 of

---

these mission-related action items entails the development of requirements for an information technology platform to support inspection activities. Another entails the development of plans to improve ISCD's site security plan review process. Regarding the latter, ISCD encountered delays approving security plans because, according to ISCD officials, the quality of the plans submitted was inconsistent and ISCD did not have dedicated staff with the skills needed to work with facilities to review and approve them. As noted in the ISCD memorandum, the site security plan review process was overly complicated, did not leverage available resources, and created bottlenecks and clearing the backlog of security plan's was ISCD's highest priority.<sup>20</sup> To address these concerns, ISCD developed an interim review process to clear the backlog of tier 1 security plans with a goal of completing reviews of those plans by the end of the calendar year. ISCD began to track the action item intended to develop a plan for introducing a new security plan review process, which, according to the June 2012 action plan, is supposed to be completed in July 2012. The development of a new security plan review process may be critical to the effective implementation of the CFATS program. According to an ISCD official, compliance inspections cannot begin until ISCD reviews and approves a facility's site security plan. In March 2012, the official estimated that it could take at least 18 months for ISCD to complete its first compliance inspections. In commenting on our draft statement, ISCD officials stated that inspections for all of the approximately 4,500 tiered facilities could take several years, contingent upon available resources.

---

<sup>20</sup>According to the ISCD memorandum, clearing the backlog of site security plans was one of the top three priorities for beginning to address the challenges facing ISCD. One of the other two was developing a chemical inspection process, which is a longer-term effort that is being addressed via the action plan, in part, by an ISCD Inspection Working Group. The remaining high-priority item dealt with efforts to address ISCD management regarding its statutory responsibilities for regulating ammonium nitrate and manage personnel surety as part of the CFATS program. Regarding the latter, personnel surety is one of the CFATS performance standards. As such, DHS requires facilities to perform background checks on and ensure appropriate credentials for facility personnel and DHS is required to check for terrorist ties by comparing certain employee information with its terrorist screening database. DHS's plan for collecting these data is currently being reviewed by the Office of Management and Budget in connection with the Paper Reduction Act. Regarding the former, DHS is responsible for regulating the sale and transfer of ammonium nitrate. 6 U.S.C. §§ 688-688i. DHS has issued a Notice of Proposed Rulemaking and currently is reviewing comments submitted in response to the notice. 76 Fed. Reg. 46,908 (Aug. 3, 2011). We will examine some of these issues as part of a new engagement dealing with DHS efforts to address mission-related issues.

---

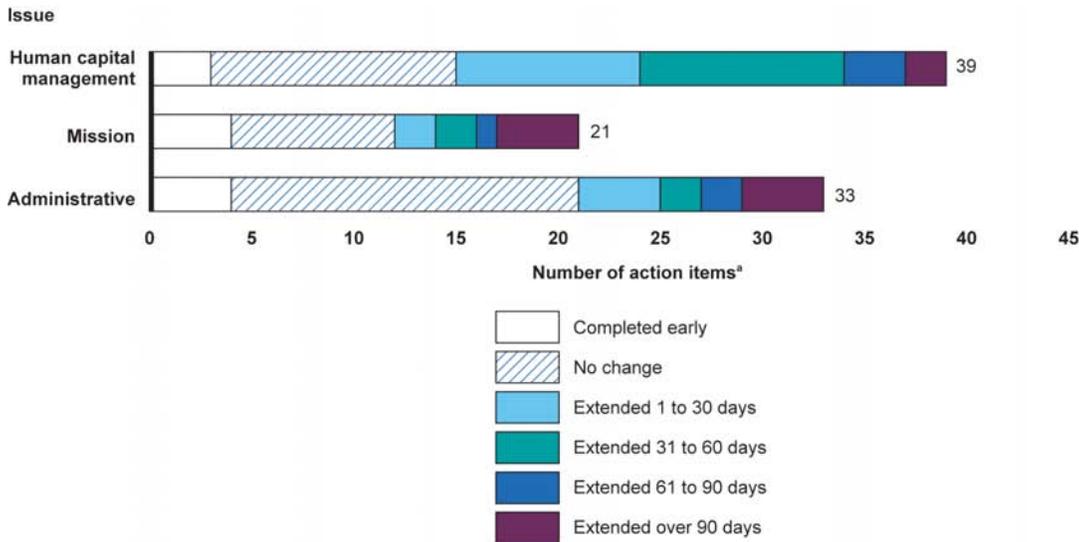
## Almost Half of ISCD's Action Item Completion Dates Have Been Extended since April 2012

Our analysis of the April and June versions of the plan shows that the division had extended the estimated completion dates for nearly half of the action items. Estimated completion dates for 52 percent (48 of 93 items)<sup>21</sup> either did not change (37 items) or the date displayed in the June 2012 plan was earlier than the date in the April 2012 version of the plan (11 items). Conversely, 48 percent (45 of 93) of the items in the June 2012 version of the plan had estimated completion dates that had been extended beyond the date in the April 2012 plan. For example, in the April 2012 plan, ISCD was to work with NPPD and IP on identifying job skills, the correct job series, and job descriptions, action that was estimated to be completed in July 2012. However, the June 2012 plan shows that the completion date for this action item was extended to August 2012, more than 30 days beyond the date estimated in April 2012. Figure 4 shows the extent to which action plan items were completed earlier than planned, did not change, or were extended, from April 2012 through June 2012, for the human capital management, mission, and administrative issues identified in the plan.

---

<sup>21</sup>ISCD data show that 93 of 94 action items were consistent between the April 2012 and June 2012 action plans; therefore, computation of the estimated completion dates is based on 93 total items. One action item in the April 2012 plan dealing with strategies for managing ISCD funding levels was removed from the June 2012 plan because after the analysis was prepared and submitted to NPPD, the decision was made to delete the item from the plan. The funding action item was replaced in the June 2012 action plan with an action item to conduct a peer review of the facility tiering process and formula. For purposes of this analysis, we use the 93 action items (instead of 94 action items) that were consistent between the April and June 2012 action plans.

**Figure 4: Changes in CFATS Action Plans Estimated Completion Dates from April 2012 to June 2012**



Source: GAO analysis of ISCD data.

<sup>a</sup>ISCD data show that 93 of 94 action items were consistent between the April 2012 and June 2012 action plans, therefore, computation of the estimated completion dates is based on 93 total items. One action item in the April 2012 plan dealing with strategies for managing ISCD funding levels was removed from the June 2012 plan because after the analysis was prepared and submitted to NPPD, the decision was made to delete the item from the plan. The funding action item was replaced in the June 2012 plan with an action item to conduct a peer review of the facility tiering process and formula. For purposes of this analysis, we use the 93 action items that were consistent between the April and June 2012 action plans.

ISCD officials told us that estimated completion dates have been extended for various reasons. They said that one reason for moving these dates was that the work required to address some items was not fully defined when the plan was first developed and as the requirements were better defined, the estimated completion dates were revised and updated. In addition, ISCD officials also stated that timelines have been adversely affected for some action items because staff have been reassigned to work on higher-priority responsibilities, such as moving staff from their assigned duties to work on efforts to reduce the backlog of security plans under review. ISCD officials also told us that some dates have been extended because the division is awaiting actions within ISCD or by NPPD or IP.

---

## Action Plan Performance Measures Could Help Gauge Progress

ISCD, through its action plan, appears to be heading in the right direction toward addressing the challenges identified, but it is too early to tell if the action plan is having the desired effect because (1) the division has only recently completed some action items and continues to work on completing more than half of the others, some of which entail long-term changes, and (2) ISCD has not developed an approach for measuring the results of its efforts. ISCD officials told us that they had not yet begun to plan or develop any measures, metrics, or other documentation focused on measuring the impact of the action plan on overall CFATS implementation because they plan to wait until corrective action on all items has been completed before they can determine the impact of the plan on the CFATS program. For the near term, ISCD officials stated that they plan to assess at a high level the impact of the action plan on CFATS program implementation by comparing ISCD's performance rates and metrics pre-action plan implementation and post-action plan implementation.<sup>22</sup> However, because ISCD will not be completing some action items until 2014, it will be difficult for ISCD officials to obtain a complete understanding of the impact of the plan on the program using this comparison only.

Now that ISCD has begun to take action to address the challenges identified, ISCD managers may be missing an opportunity to measure the effects or results of some of the actions taken thus far, particularly actions that are either in the early stages of implementation or are in the formative stages. Measuring results associated with particular action items would be consistent with *Standards for Internal Control in the Federal Government*, which calls for the establishment and review of performance measures and indicators to monitor activities and compare actual performance with planned or expected results throughout the organization and analyze significant differences. We recognize that it might not be practical to establish performance measures for all action items, for example; 1 of the 94 items calls for ISCD to initiate the hiring process for an economist. However, other action items may be candidates for performance measurement because they focus on organizational changes or mission-related issues. For example, once ISCD gets approval to move forward with a plan to reorganize, it could

---

<sup>22</sup>According to NPPD officials, ISCD uses performance measures to track the performance of the CFATS program overall, but as of June 2012 did not have performance measures in place to track the progress of the action plan, or particular action items.

---

develop interim plans and measures to monitor the progress of integrating various functions and use the information to identify barriers, if any, for completing this effort. Likewise, once ISCD makes the decision to revise its site security plan review process, it could develop measures for implementing those revisions and consider what measures might be appropriate for gauging its success in streamlining the process and completing security plan reviews. By looking for opportunities to develop performance measures covering the various action items and developing such measures, ISCD managers would be better positioned to identify any gaps in their efforts to address the challenges and have tools available to measure and monitor performance in the future. ISCD would also have a framework for providing continuity of operations when new managers or staff are hired, managers move from position to position, or as the program changes. Furthermore, ISCD would be better equipped to inform stakeholders of its progress as the organization moves toward resolving the challenges identified in the ISCD memorandum.

---

## **ISCD Officials Stated That Almost Half of the Action Items Require Collaboration with or Action by NPPD or IP**

According to ISCD officials, almost half of the action items included in the June 2012 action plan either require ISCD to collaborate with NPPD and IP or require NPPD and IP to take action to address the challenges identified in the ISCD memorandum. NPPD, IP, and ISCD officials have been working together to identify solutions to the challenges the memorandum identified and to close pertinent action items.

One of the issues identified in the ISCD memorandum was the level of NPPD and IP communication and support. According to ISCD officials, at the time the program was established, NPPD and IP communication and support were not adequate for the division to implement the CFATS program within the statutory time frames (which was 6 months following the passage of the CFATS statute). Regarding the ISCD memorandum and the action plan, NPPD, IP, and ISCD officials have been working together to identify solutions to these human capital and administrative challenges. According to division officials, 46 of the 94 action items included in the June 2012 action plan require either action by NPPD and IP or collaboration with NPPD and IP. This includes collaborating with NPPD officials representing the NPPD human capital, facilities, and employee and labor relations offices, among others, and with IP's

---

Directorate of Management Office.<sup>23</sup> As of June 2012, 13 of the 46 items that require action by or collaboration with NPPD or IP are complete; 33 of 46 are in progress.

With regard to completed items, these focused largely on human capital and administrative issues. For example, 1 completed item required ISCD leaders to establish regular meetings with NPPD and IP human capital officials to ensure better communication and visibility on human capital issues. Our discussions with ISCD and NPPD officials confirmed that this action item was closed because meetings covering human capital issues have begun and are held on a weekly and recurring basis. NPPD, IP, and ISCD told us that one of the topics of discussion during the weekly meetings is the hiring of specialists so that the division has assurance that the CFATS reviews and inspection process properly include their expertise. According to these officials, hiring certain types of specialists is a difficult challenge given that ISCD is competing with other organizations, including organizations within DHS, for individuals that possess these specialized skills. These officials also stated that these weekly meetings provide NPPD, IP, and ISCD an opportunity to discuss human capital issues as they come up and ensure that the division's hiring process runs smoothly. To further assist with ISCD's hiring efforts, IP officials said that one IP human capital staff member is moving to be co-located with the division with the intent that this co-located staff member will be an important accelerator to the hiring process and help keep ISCD hiring on track. Another related action item required similar meetings between ISCD and NPPD's Office of Employee and Labor Relations to discuss union-related issues. This item was closed because these NPPD staff members meet weekly with ISCD senior leaders to discuss how the union operates and how they should work with the union, and help them understand and properly address the division's obligations to the union.

With regard to the 33 of 46 actions items requiring collaboration with NPPD and IP that are in progress, 23 require NPPD or IP to review and approve work completed by ISCD or make policy decisions before the division can list the action item as complete. For example,

---

<sup>23</sup>The IP Directorate of Management Office is responsible for providing IP divisions with program management support such as training and facilities management.

- 
- Twelve of the 33 action items involve ISCD's development of the aforementioned realignment plan. As of June 2012, ISCD had forwarded the realignment plan to NPPD and IP for review and was awaiting approval so that the plan could be forwarded to DHS for review and comment.
  - Another action item requires ISCD to develop a human capital strategic plan. According to the June 2012 action plan, ISCD is waiting for NPPD to release its Human Capital Strategic Plan to finalize this action item and plans to use the guidance provided in the NPPD plan to develop an ISCD Strategic Human Capital Plan.

ISCD continues to work on the remaining 10 of the 33 in-progress action items that require NPPD or IP action or division collaboration with NPPD and IP. According to the June 2012 action plan, completion of these action items is dependent upon ISCD staff completing an internal review of an ISCD-drafted set of standard operating procedures or memorandum, or an analysis of an existing ISCD procedure. Once ISCD finalizes these 10 action items, the outputs are to be forwarded to NPPD and IP for review, comment, and approval, where appropriate.

Additional details on action items that require collaboration with or action by NPPD or IP are considered "for official use only."

---

## Conclusions

ISCD has identified numerous challenges it has encountered implementing the CFATS program and has developed an action plan that is intended to help address these challenges. This appears to be a step in the right direction as officials continue their efforts to better manage the program and establish a viable process consistent with the statute and the CFATS rule. Because of the scope and breadth of the action plan and given that many of the action items were recently completed (38 of 94 action items) or are in progress (56 of 94 action items), it is too early to tell whether they will have the effect of helping ISCD overcome and resolve all the problems it has identified. However, ISCD, working with NPPD and IP, may be better positioned to understand and report on its progress by looking for opportunities to measure the effect of efforts to implement key action items, especially since many of the action items are either recently completed or in their formative stages. By developing performance measures, where practical, ISCD, IP, and NPPD would be better equipped to identify any gaps between actual and planned or expected results and take corrective action, where necessary, consistent with *Standards for Internal Control in the Federal Government*.

---

Furthermore, ISCD, IP, and NPPD would be better positioned to report on their progress developing a viable CFATS program to key stakeholders, including Congress.

---

## Recommendation for Executive Action

To better ensure that DHS can better understand the effect of its actions as it moves forward with its efforts to address the challenges facing ISCD as it implements the CFATS program, we recommend that the Secretary of Homeland Security direct the Under Secretary for NPPD, the Assistant Secretary for IP, and the Director of ISCD, in conjunction with the development of ISCD's strategic plan, to look for opportunities, where practical, to measure results of their efforts to implement particular action items, and where performance measures can be developed, periodically monitor these measures and indicators to identify where corrective actions, if any, are needed.

---

## Agency Comments and our Evaluation

We provided a draft of this statement to the Secretary of Homeland Security for review and comment. The Deputy Under Secretary for NPPD and the Assistant Secretary for Infrastructure Protection provided oral comments on July 23, 2012, and stated that NPPD agreed with our recommendation. NPPD officials said that they intend to provide an updated action plan that includes a new action item to "develop metrics for measuring, where practical, results of efforts to implement action plan items, including processes for periodic monitoring and indicators for corrective actions." The Deputy Under Secretary also noted that these new measures would be in addition to the program metrics NPPD uses to measure the overall progress of the CFATS program.

DHS also provided technical comments, which we incorporated as appropriate.

---

As agreed with your offices, we will continue to review the CFATS program and review ISCD's efforts to manage the mission aspects of the program. This will include ISCD efforts to determine chemical facility risk; manage the process used to assess vulnerabilities, review security plans, and perform inspections; and work with owners and operators of high-risk chemical facilities. We expect to report the results of these efforts early in 2013.

---

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

---

## GAO Contact and Staff Acknowledgements

For information about this statement please contact Stephen L. Caldwell, Director, Homeland Security and Justice, at (202) 512-8777 or [CaldwellS@gao.gov](mailto:CaldwellS@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals making key contributions include John F. Mortin, Assistant Director; Ellen Wolfe, Analyst-in-Charge; Charles Bausell; Jose Cardenas; Andrew M. Curry; Michele Fejfar; Tracey King; Marvin McGill; Mona E. Nichols-Blake; and Jessica Orr.

---

# Appendix I: Objectives, Scope and Methodology

---

This statement discusses how the internal Infrastructure Security Compliance Division's (ISCD) memorandum (the ISCD memorandum) was developed and what challenges were identified, what actions are being taken to address the challenges identified, and the extent to which ISCD's planned actions and proposed solutions require collaboration with National Protection and Programs Directorate (NPPD) or the Office of Infrastructure Protection (IP).

To determine how the ISCD memorandum was developed and the challenges outlined in the memorandum, we reviewed and analyzed the memorandum to determine the various Chemical Facility Anti-Terrorism Standards (CFATS) program challenges as identified by the memorandum's author—i.e., the ISCD Director, who was the primary author, in consultation with the Deputy Director. As a part of our analysis, we grouped the challenges into overarching categories—human capital management issues, mission issues, and administrative issues—and used the sub-categories developed by the author of the ISCD memorandum to summarize the types of challenges or problems described in the ISCD memorandum. We also interviewed 14 ISCD senior officials (including the ISCD Director and Deputy Director) to confirm our understanding of the challenges identified, determine how the memorandum was developed, and obtain ISCD officials' views on what may have created the CFATS program challenges.

To determine what actions ISCD is taking to address the challenges identified in the memorandum, we analyzed and compared the various action plans that were prepared by ISCD senior officials between January 2012 and June 2012. We developed a list of the 94 action items included in the June plan and determined the status of each action item (completed or in progress), the extent to which the ISCD officials responsible for leading efforts for the action item agreed that the action item addressed an existing problem, and the extent to which the activities related to the action item were in progress prior to the ISCD memorandum's release. Where possible, we obtained and reviewed documentation (e.g., standard operating procedures and ISCD memos) relevant to each action item to support ISCD officials' views that the status of the action item was accurate and whether the work on the action item was in progress before the development and release of the ISCD memorandum. We also compared the results of our analysis of the action plans and our discussions with program officials with various criteria, including the CFATS law and regulations; Department of Homeland Security (DHS) policies, procedures, and reports; *Standards for Internal*

---

*Control in the Federal Government*,<sup>1</sup> and *The Standard for Program Management*.<sup>2</sup>

To determine the extent to which ISCD's planned actions and proposed solutions require collaboration with or action by NPPD or IP officials, we interviewed 11 NPPD and 9 IP officials identified by ISCD officials who are to work with ISCD to implement corrective actions. Using the results of these interviews and our analysis of the ISCD memorandum and action plan, we determined the extent to which collaboration among ISCD, NPPD, and IP is required to implement corrective action, if at all. Where available, we obtained and reviewed NPPD, IP, and ISCD documentation (e.g., policies, standard operating procedures, and internal memos) relevant to each action item that requires NPPD or IP support or action in working with ISCD to overcome those challenges.

We identified three limitations that should be considered when using our results. First, ISCD's memorandum is largely based on the efforts of the ISCD Director in consultation with the ISCD Deputy Director and may not be representative of the views of other senior officials within the CFATS program. Furthermore, the conclusions reached in the memorandum were not obtained by using a formal compliance audit or program review procedures, nor were the assumptions validated. Second, our results are based on the status of the action plan as of June 2012, so these results are valid only up until this point in time. Third, documentary evidence about the development of the CFATS program and the causes for the issues identified in the ISCD memorandum is, for the most part, not available. Program officials did not maintain records of key decisions and

---

<sup>1</sup>GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD 00-21.3.1 (Washington, D.C.: November 1999). Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, the Office of Management and Budget issued Circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government*.

<sup>2</sup>Project Management Institute, *The Standard for Program Management*© (Newtown Square, Pa: 2006). *The Standard for Program Management* provides guidelines for successfully managing programs and projects.

the basis for those decisions during the early years of the program. During preliminary discussions, the members of current management team qualified that much of their knowledge about program decisions during the early years of the program is their best guess of what happened and why.

We conducted this performance audit from February 2012 to July 2012 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 analysis based on our audit objectives.

---

# Appendix II: ISCD Organizational Structure within NPPD and IP as of June 2012

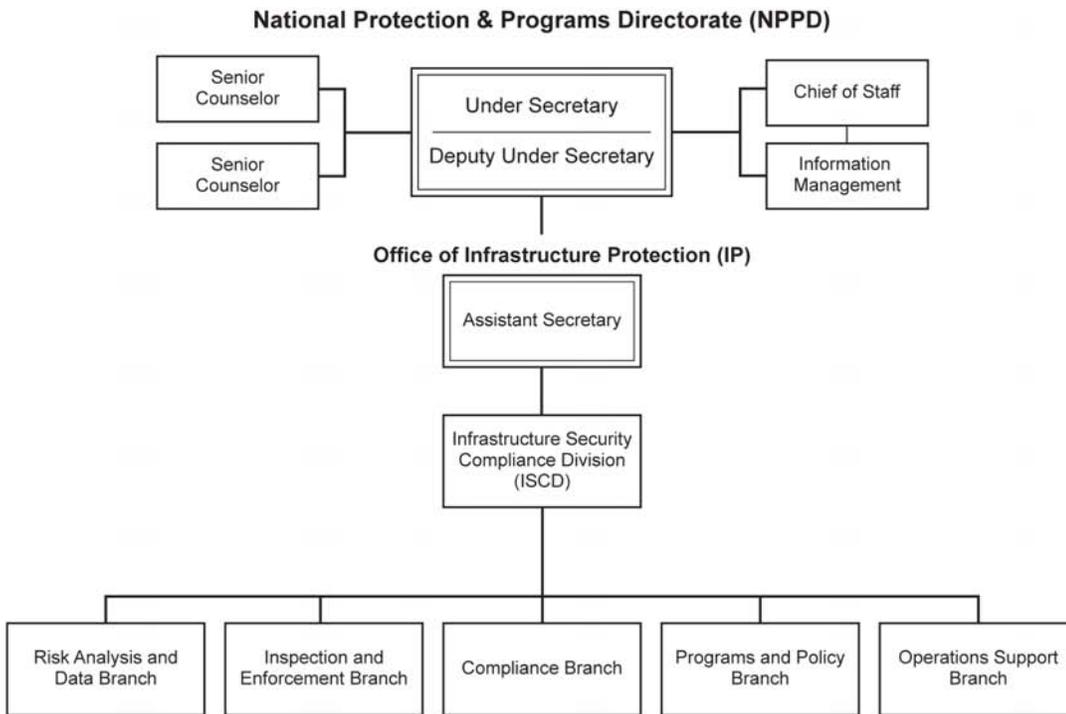
---

This appendix provides the organizational structure used to manage the Chemical Facility Anti-Terrorism Standards program within the Infrastructure Security Compliance Division. ISCD has direct responsibility for implementing DHS's CFATS rule, including assessing high-risk chemical facilities, promoting collaborative security planning, and ensuring that covered facilities meet DHS's risk-based performance standards.<sup>1</sup> ISCD is managed by a Director and a Deputy Director and operates five branches that are, among other things, responsible for information technology operations; policy and planning; providing compliance and technical support; inspecting facilities and enforcing CFATS regulatory standards; and managing logistics, administration, and chemical security training. ISCD receives business support from the National Protection and Programs Directorate and the Office of Infrastructure Protection for services related to human capital management and training, budget and finance, and acquisitions and procurement. Figure 5 shows the organizational structure of NPPD, IP, and ISCD.

---

<sup>1</sup>The CFATS rule establishes 18 risk-based performance standards that identify the areas for which a facility's security plan is 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 they achieve the requisite level of performance in each of the applicable areas.

Figure 5: ISCD Organizational Structure within NPPD and IP as of June 2012



Source: GAO analysis of NPPD, IP, and ISCD organizational charts.

# Appendix III: Summary of ISCD Action Plan by Issue and Subcategory, and Status

This appendix provides a summary of the status and progress of action items grouped by issue and sub-category. The Infrastructure Security Compliance Division is using an action plan to track its progress in addressing the challenges identified in the November 2011 ISCD memorandum prepared by the ISCD Director in consultation with the Deputy Director. The ISCD memorandum was accompanied by an action plan that, according to the authors of the memorandum, was intended to provide solutions to addressing the challenges identified. Table 1 provides an overview of the items in the action plan and their status (completed or in progress) by issue (human capital management, mission issues, and administrative issues) and subcategory.

**Table 1: Summary of ISCD Action Items by Overarching Issues and Subcategory and Status, June 2012**

Issue	Sub-category	Overview of action items	Number of action items in progress	Number of action items complete	Total number of action items
Human capital management			13	17	30
	Culture	Action items in this category are intended to improve overall communication within the division between staff and management, develop procedures for addressing conduct and discipline issues, and enhance employee awareness about policies and procedures to address conduct and discipline.	1	10	11
	Performance	Action items in this category are intended to assist in the development of ISCD's performance management procedures and training and to ensure DHS, NPPD, and IP performance policies and procedures are communicated to all employees.	2	1	3
	Staffing	Action items in this category are intended to address ISCD's efforts to conduct an organizational realignment of staff; hire employees to fill skill and experience gaps; upgrade employee skills consistent with ISCD's mission; and train employees in conduct, discipline, and performance issues.	10	3	13
	Union	Action items in this category are intended to focus on ISCD's efforts to address union-related issues, including efforts to coordinate with the union on employee and labor issues.	0	3	3

**Appendix III: Summary of ISCD Action Plan by Issue and Subcategory, and Status**

<b>Issue</b>	<b>Sub-category</b>	<b>Overview of action items</b>	<b>Number of action items in progress</b>	<b>Number of action items complete</b>	<b>Total number of action items</b>
<b>Mission</b>					
		Action items in this category are intended to address issues associated with the CFATS program core mission activities, including efforts to streamline the site security plan review process and develop processes and procedures for conducting inspections at tiered facilities.	16	6	<b>22</b>
<b>Administrative</b>			<b>27</b>	<b>15</b>	<b>42</b>
	Contracting	Action items in this category are intended to address concerns about ISCD's reliance on contractors to support mission-essential activities and assess whether inherently governmental activities are being performed by contractors.	3	4	<b>7</b>
	Documentation	Action items in this category are intended to focus on the development of a human capital strategic plan, and address deficiencies in ISCD's records management system and various administrative policies and procedures.	11	5	<b>16</b>
	Human resources	Action items in this category address ISCD, IP, and NPPD communications and collaboration regarding human capital issues, such as hiring qualified staff and employee and labor relations, and ISCD's efforts to reassign personnel to better achieve CFATS mission goals.	5	4	<b>9</b>
	Inspector	Action items in this category are intended to address concerns about vehicle use, administratively uncontrollable overtime, and other administrative issues pertaining to CFATS inspectors.	3	2	<b>5</b>
	Miscellaneous	Action items in this category are intended to focus on ISCD's organizational alignment, clarify functions within the organization, and equipment requirements for CFATS inspectors.	3	0	<b>3</b>
	Property management	This action item is intended to focus on ISCD's reduced requirement for classified space.	1	0	<b>1</b>
	Real estate	This action item is intended to focus on ISCD's field operation space requirements.	1	0	<b>1</b>
<b>Total</b>			<b>56</b>	<b>38</b>	<b>94</b>

Source: GAO analysis of June 2012 ISCD action plan prepared by ISCD officials.

---

# Related GAO Products

---

*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 Protection: Sector Plans Complete and Sector Councils Evolving.* [GAO-07-1075T](#). Washington, D.C.: July 12, 2007.

*Critical Infrastructure Protection: Sector Plans Complete 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.

*Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges.* [GAO-05-327](#). Washington, D.C.: March 28, 2005.

---

---

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

