

Department of Homeland Security **Office of Inspector General**

Effectiveness of the Infrastructure Security
Compliance Division's Management Practices to
Implement the Chemical Facility Anti-Terrorism
Standards Program



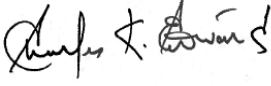


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

March 25, 2013

MEMORANDUM FOR: The Honorable Rand Beers
Undersecretary
National Protection and Programs Directorate

FROM: Charles K. Edwards 
Deputy Inspector General

SUBJECT: *Effectiveness of the Infrastructure Security Compliance
Division's Management Practices to Implement the
Chemical Facility Anti-Terrorism Standards Program*

Attached for your information is our final report, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program*. We incorporated the formal comments from the National Protection and Programs Directorate in the final report.

The report contains 24 recommendations aimed at improving the Chemical Facility Anti-Terrorism Standards Program. Your office concurred with 19 recommendations, partially concurred with 1 recommendation, and did not concur with 4 recommendations. Based on information provided in your response, we consider Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, and 25 to be open and resolved; however, Recommendation 19 is open and unresolved.

As prescribed by the Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for the Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered resolved and open.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Please call me with any questions, or your staff may contact
Deborah L. Outten-Mills, Acting Assistant Inspector General for Inspections, at
(202) 254-4015, or Marcia Moxey Hodges, Chief Inspector, at (202) 254-4202.

Attachment



Table of Contents

Executive Summary.....	1
Background	3
Results of Review	13
CFATS Program Tools Need Modification To Improve Efficiency, Effectiveness, and Utility.....	13
Recommendations	15
Management Comments and OIG Analysis	16
SSP Review Process Has Hindered CFATS Program Progress	17
Recommendations	23, 25, 27
Management Comments and OIG Analysis	23, 25, 27
Management of the Personnel Surety Program Resulted in Premature Expenditure of Funds	27
Recommendation.....	31
Management Comments and OIG Analysis	31
Congress Provided ISCD Additional Chemical Security Regulatory Responsibility	31
Recommendations	33
Management Comments and OIG Analysis	33
Confusing Terminology and Absence of Appropriate Metrics Led To Misunderstandings of CFATS Program Progress	34
Recommendation.....	39
Management Comments and OIG Analysis	39
IP, NPPD, Congress, and DHS OIG Provided Limited Oversight of ISCD and the CFATS Program.....	40
Recommendation.....	43
Management Comments and OIG Analysis	43
Overall Coordination, Communication, and Actions Taken To Address Facility Tiering Methodology Errors Were Ineffective, and Concerns Remain That Tiering Is Still Flawed.....	46
Recommendations	50



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Management Comments and OIG Analysis	50
Pressure To Implement the CFATS Program Led ISCD To Rely on Contractor Support.....	51
Recommendation.....	54
Management Comments and OIG Analysis	55
ISCD Struggles To Provide Employees With Appropriate Training	55
Recommendation.....	57
Management Comments and OIG Analysis	57
Inability To Follow Sound Government Practices Has Resulted in Noncompliance and Wasted Resources.....	58
Recommendations	62, 71, 76
Management Comments and OIG Analysis	62, 71, 76
Dysfunctional Culture Contributed to Perceptions of Retaliation and Suppression of Nonconforming Opinions Within ISCD	78
Recommendations	79
Management Comments and OIG Analysis	80
NPPD Has a Process To Report Allegations, but DHS OIG Contact Information Is Outdated	80
Recommendation.....	81
Management Comments and OIG Analysis	81
Industry Supports the CFATS Program, but Challenges Remain and Corrective Action Is Necessary	82
Recommendation.....	84
Management Comments and OIG Analysis	84
Conclusion.....	85

Appendixes

Appendix A: Objectives, Scope, and Methodology.....	86
Appendix B: Recommendations.....	88
Appendix C: Management Comments to the Draft Report	92
Appendix D: ISCD Field Locations, Staff, and Regulated Facilities.....	109
Appendix E: F1 Factor Timeline of Events.....	110
Appendix F: F1 Communication to IP Leadership and NPPD Staff.....	111



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix G: Designation of Leadership Positions in IP 112
Appendix H: Major Contributors to This Report 113
Appendix I: Report Distribution 114

Abbreviations

ASP	Alternative Security Program
AUO	Administratively Uncontrollable Overtime
CAV	Compliance Assistance Visit
CFATS	Chemical Facility Anti-Terrorism Standards
COI	Chemical of Interest
CSAT	Chemical Security Assessment Tool
DHS	Department of Homeland Security
FPS	Federal Protective Service
FRC	Federal Review Center
FY	fiscal year
GAO	Government Accountability Office
GS	General Schedule
IP	Office of Infrastructure Protection
ISCD	Infrastructure Security Compliance Division
NPPD	National Protection and Programs Directorate
OCS	Office of Compliance and Security
OGC	Office of General Counsel
OIG	Office of Inspector General
OPM	Office of Personnel Management
RBPS	risk-based performance standards
SSP	Site Security Plan
SVA	Security Vulnerability Assessment
TSA	Transportation Security Administration
TSDB	Terrorist Screening Database
TSC	Terrorist Screening Center
TWIC	Transportation Worker Identification Credential
USCG	U.S. Coast Guard



Executive Summary

The *Department of Homeland Security Appropriations Act of 2007* established the Chemical Facility Anti-Terrorism Standards Program, which allows the Department of Homeland Security (DHS) to regulate chemical facilities that may present a high-level security risk. Within the Department's National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection, the Infrastructure Security Compliance Division is responsible for implementing the Chemical Facility Anti-Terrorism Standards Program.

In December 2011, a limited distribution internal memorandum was leaked to news media. This document disclosed allegations of employee misconduct and inadequate performance, as well as misuse of funds and ineffective hiring within DHS' Chemical Facility Anti-Terrorism Standards Program. In February 2012, former Chairman Lungren, of the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, requested that we review these issues. In April 2012, Ranking Member Waxman, of the House Committee on Energy and Commerce, also requested that we review the challenges facing the program. We consolidated both requests into one review.

We assessed DHS' efforts to implement the Chemical Facility Anti-Terrorism Standards Program from inception to the end of fiscal year 2012. Specifically, we reviewed whether: (1) management controls are in place and operational to ensure that the Chemical Facility Anti-Terrorism Program is not mismanaged; (2) NPPD and Infrastructure Security Compliance Division leadership misrepresented program progress; and (3) nonconforming opinions of program personnel have been suppressed or met with retaliation.

Program progress has been slowed by inadequate tools, poorly executed processes, and insufficient feedback on facility submissions. In addition, program oversight had been limited, and confusing terminology and absence of appropriate metrics led to misunderstandings of program progress. The Infrastructure Security Compliance Division still struggles with a reliance on contractors and the inability to provide employees with appropriate training. Overall efforts to implement the program have resulted in systematic noncompliance with sound Federal Government internal controls and fiscal stewardship, and employees perceive that their opinions have been suppressed or met with retaliation. Although we were unable to substantiate any claims of retaliation or suppression of nonconforming opinions, the Infrastructure Security Compliance Division work environment and culture cultivates this perception. Despite the Infrastructure Security Compliance Division's challenges, the regulated community views the Chemical Facility Anti-Terrorism Standards Program as necessary



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

in establishing a level playing field across a diverse industry. We are making 24 recommendations to correct these deficiencies and attain intended program results and outcomes. The Infrastructure Security Compliance Division concurred with 19 recommendations, partially concurred with 1 recommendation and did not concur with 4.



Background

Chemical Facility Anti-Terrorism Standards Program History

After the 2001 terrorist attacks, the Nation developed a greater awareness of potential terrorist targets. For example, chemical facilities became viewed as potentially attractive to terrorists because these facilities could be sabotaged and materials released, stolen, or used as weapons of mass destruction.

Even an accidental chemical release can be disastrous, as illustrated in January 2005, when two trains collided and derailed in Graniteville, SC. This accident caused one railcar carrying 90 tons of chlorine gas to rupture, resulting in nine deaths and displacing 5,400 people for 2 weeks. In October 2012, a hydrochloric acid leak created a vapor cloud that drifted over the population of Texas City, TX, injuring nine people. Both accidents occurred in lightly populated areas; an intentional terrorist release of toxic gas in a densely populated area could result in potential catastrophic death and injury. Recognizing this risk, many chemical companies initiated security programs and made significant capital investments to address security concerns. In addition, several States adopted measures to enhance the security of chemical facilities under their jurisdiction.

Congressional Action and Placement of Regulatory Authority Within DHS

To address these concerns, Congress, in Section 550 of the *Department of Homeland Security Appropriations Act of 2007*, Public Law 109-295, granted DHS authority to regulate the security of high-risk chemical facilities.¹ DHS assigned this responsibility to NPPD. NPPD is responsible for leading the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Within NPPD, the Office of Infrastructure Protection (IP) leads the coordinated national program to reduce risks to the Nation's critical infrastructure. This infrastructure is defined as the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health, or safety. In October 2006, IP's Assistant Secretary established the

¹ Facilities exempt from this act are those regulated by the United States Coast Guard pursuant to the *Maritime Transportation Security Act*, drinking water and wastewater treatment facilities as defined by Section 1401 of the *Safe Water Drinking Act* and Section 212 of the *Federal Water Pollution Control Act*, and facilities owned or operated by the Departments of Defense and Energy, as well as certain facilities subject to regulation by the Nuclear Regulatory Commission.



Chemical Security Working Group to perform the regulatory, organizational, and resource planning necessary to implement the legislative mandate of regulating the Nation’s chemical facilities. This working group established the Chemical Security Compliance Project to develop the regulatory framework and associated tools and procedures to implement and ensure facility compliance.

Developing the Program’s Regulatory Framework and Structure

In February 2007, IP’s Assistant Secretary established the Chemical Security Compliance Division. The mission of the Chemical Security Compliance Division was to achieve initial operating capability of the Chemical Security Compliance Project and to reach full operating capability by October 2009. In November 2007, the division was renamed the Infrastructure Security Compliance Division (ISCD), but the mission did not change.

To comply with the requirements of the *Appropriations Act of 2007*, DHS published the Chemical Facility Anti-Terrorism Standards (CFATS) Interim Final Rule in the *Federal Register* on April 9, 2007.² The Interim Final Rule established the program’s risk-based performance standards (RBPS) that all facilities must satisfy; however, measures sufficient to meet these standards are more rigorous for facilities that present higher levels of risk. Table 1 lists the 18 RBPS.

Table 1: CFATS Program RBPS and Descriptions

Risk-Based Performance Standards	Descriptions
1 Restrict Area Perimeter	Secure and monitor the perimeter of the facility.
2 Secure Site Assets	Secure and monitor restricted areas or potentially critical targets within the facility.
3 Screen and Control Access	Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter.
4 Deter, Detect, and Delay	Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful.
5 Shipping, Receipt, and Storage	Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.
6 Theft and Diversion	Deter theft or diversion of potentially dangerous chemicals.
7 Sabotage	Deter insider sabotage.

² *Chemical Facility Anti-Terrorism Standards; Interim Final Rule*, 72 FR 17688, April 9, 2007.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Risk-Based Performance Standards		Descriptions
8	Cyber	Deter cyber sabotage, to include preventing unauthorized onsite or remote access to critical process controls.
9	Response	Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.
10	Monitoring	Maintain effective monitoring, communications, and warning systems.
11	Training	Ensure proper security training, exercises, and drills of facility personnel.
12	Personnel Surety	Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets.
13	Elevated Threats	Escalate the level of protective measures for periods of elevated threat.
14	Specific Threats, Vulnerabilities, or Risks	Address specific threats, vulnerabilities, or risks identified by the Assistant Secretary for the particular facility at issue.
15	Reporting of Significant Security Incidents	Report significant security incidents to the Department and to local law enforcement officials.
16	Significant Security Incidents and Suspicious Activities	Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site.
17	Officials and Organization	Establish official(s) and an organization responsible for security and for compliance with these standards.
18	Records	Maintain appropriate records.

Source: May 2009 Risk-Based Performance Standards Guidance, CFATS.

The Interim Final Rule went into effect on June 8, 2007, but allowed for further public comment on the proposed appendix A. This appendix included a tentative list of Chemicals of Interest (COIs) that DHS identified as having the potential to create significant human life and/or health consequences if released, stolen or diverted, and/or contaminated. DHS revised appendix A, which includes the final comprehensive list of COIs and a screening threshold quantity for each COI, which when present at a facility requires an initial submission of site information for CFATS Program consideration. Appendix A went into effect on November 20, 2007.



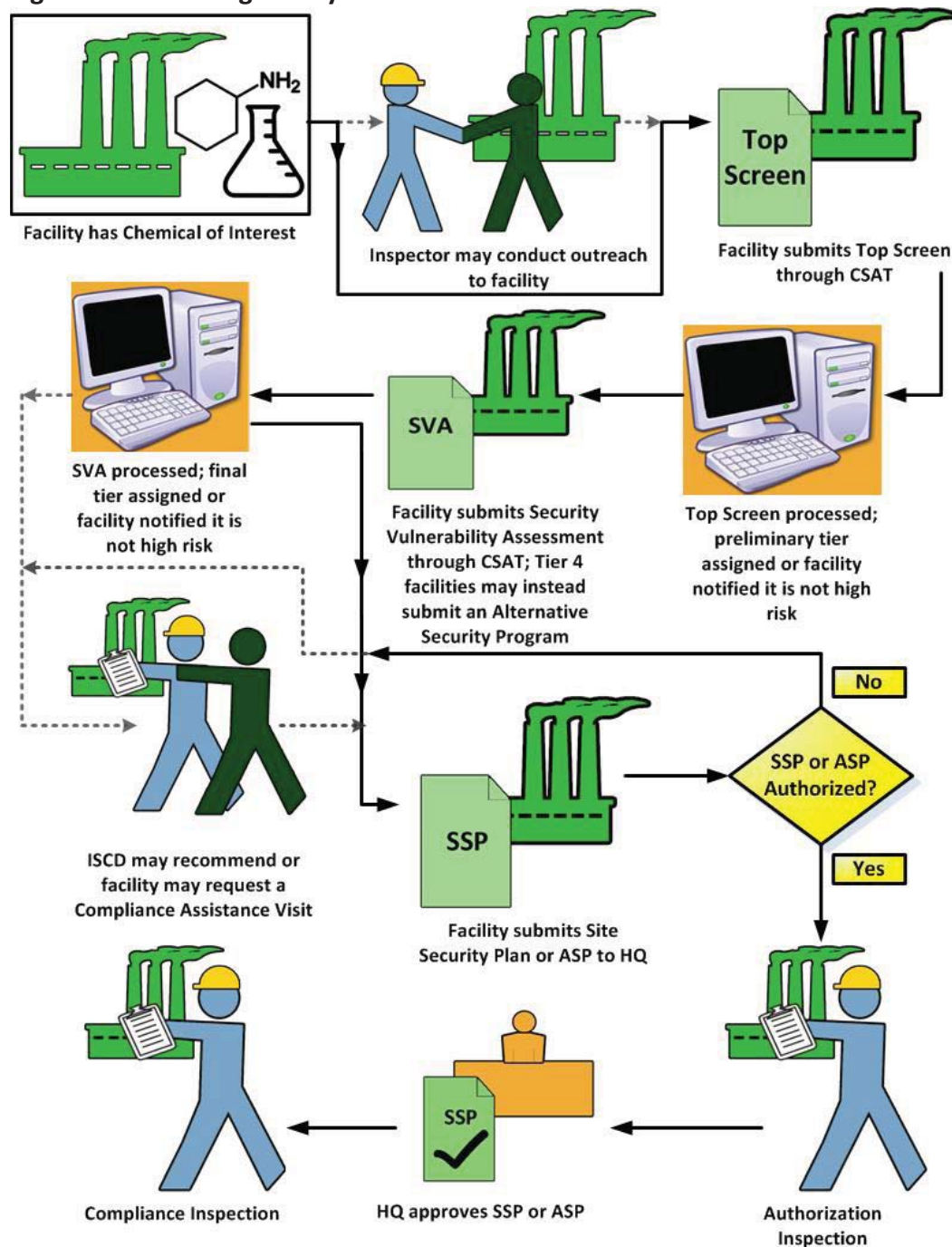
Determining Facility Risk

To determine risk, the CFATS Program considers a number of factors, including the chemicals possessed by the facility, the quantity of those chemicals, the manner in which those chemicals are possessed, and the geographic location of the facility. Based on these factors, the Department determines whether a facility is high risk, and if so, the facility is then placed in one of four risk-based tiers, with Tier 1 containing the highest-risk facilities and Tier 4 containing lowest-risk facilities. Figure 1 represents the CFATS regulatory process.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 1: CFATS Regulatory Process³



Source: Office of Inspector General (OIG) analysis.

³ Facilities register and submit their Top Screens, Security Vulnerability Assessments (SVAs), and Site Security Plans (SSPs) or Alternative Security Programs (ASPs) online through the Chemical Security Assessment Tool (CSAT) for ISCD review and approval.



To determine tier placement, the presence of a COI in quantities above the screening threshold quantity at a facility requires the facility to submit a Top Screen. A Top Screen solicits answers to a series of questions regarding COI manufacture, storage, use, and quantities, among other things. Top Screen results assist CFATS in determining whether a facility presents a high-level security risk. After processing a Top Screen, the CFATS Program assigns the facility a preliminary tier or determines that the facility does not meet the criteria for CFATS regulation. A facility that is not determined to be high-risk is considered unregulated, but must submit a new Top Screen if it later possesses another COI at or above the applicable screening threshold quantity.

When a facility receives a preliminary tier assignment notification, it must prepare a Security Vulnerability Assessment (SVA) within 90 calendar days. The SVA requires a facility to identify onsite assets; apply specified threat scenarios to each asset to quantify the consequences if an attack succeeded; and apply threat scenarios to each asset in light of the security measures in place and evaluate the likelihood and the degree to which the attack could succeed. Tier 4 facilities may submit an Alternative Security Program (ASP) in lieu of an SVA. An ASP may be based on a third-party or industry organization program, a local authority, State or Federal Government program, or any element thereof, that IP's Assistant Secretary has determined meets CFATS requirements.⁴ After reviewing the SVA or ASP, the CFATS Program determines a facility's final tier assignment or that the facility is not high risk.

Facility Requirements After Receiving a Risk Tier Assignment

When a facility receives a final tier assignment notification, it is required to submit a Site Security Plan (SSP) within 120 calendar days. The SSP must identify and describe measures the facility will employ to address each vulnerability area. Focusing on those vulnerable areas, the SSP must then address specific potential terrorist attack modes and how each would be deterred or otherwise addressed. In addition, the SSP must identify how layered security measures selected by the facility address the RBPS. In lieu of an SSP, facilities may submit an ASP.

The CFATS Program reviews the SSPs and ASPs to determine whether the plans satisfy the RBPS and should be authorized or whether the facility needs to take further action. Chemical Security Inspectors conduct an Authorization Inspection at a facility to validate an authorized SSP or ASP. Following this inspection, the CFATS Program determines whether to approve or disapprove the SSP or ASP. DHS can disapprove a plan that does not address the vulnerability assessment

⁴ 6 CFR Subpart A, § 27.105.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

and RBPS; however, DHS cannot be prescriptive and disapprove a plan based on the presence or absence of a particular security measure. Once an SSP or ASP is approved, inspections are conducted at the facility to assess compliance with CFATS; the frequency of Compliance Inspections may vary according to a facility's tier level. The regulation then requires that Tier 1 and 2 facilities submit new Top Screens every 2 years. Facilities in Tiers 3 and 4 must resubmit Top Screens every 3 years.

Facilities are also required to resubmit a Top Screen when there are changes to operations or sites, referred to in the CFATS regulation as "material modifications," within 60 days of completion.⁵ Based on this information, the CFATS Program will determine the need for updated SVAs and SSPs. A facility may seek a redetermination by filing a request with IP's Assistant Secretary.⁶ The regulation requires the Department to send the facility a decision within 45 days.

Tools Used To Submit Facility Information to CFATS

To implement the CFATS Program, ISCD began working with the Department of Energy's national laboratories in Fall 2006 to create an online submission tool, the Chemical Security Assessment Tool (CSAT). Facilities register and submit their Top Screens, SVAs, and SSPs or ASPs through the CSAT for ISCD review and approval.

CFATS Program Management

ISCD manages and implements the CFATS Program to identify and assess high-risk chemical facilities, promote effective security planning, and help facilities reduce security risk. The ISCD Director and Deputy Director oversee five branches that assist in implementing ISCD's mission and operations, as shown in figure 2.

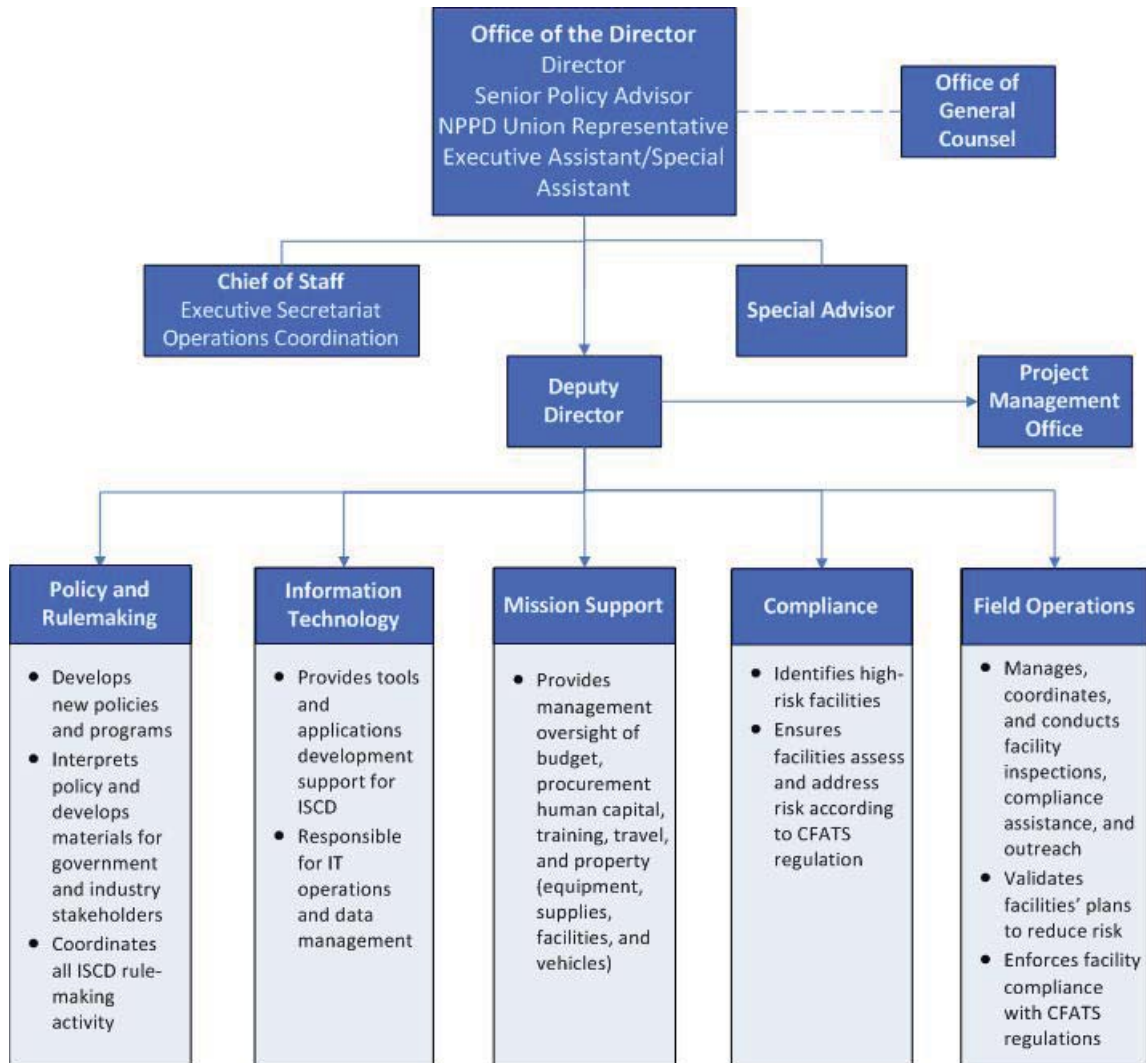
⁵ *Chemical Facility Anti-Terrorism Standards; Interim Final Rule*, 72 FR 17702, April 9, 2007.

⁶ A redetermination may occur when a regulated facility materially alters operations and seeks a decision regarding its inclusion in the CFATS Program.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 2: ISCD Organization Chart



Source: NPPD.

After our fieldwork ended in October 2012, ISCD was implementing a divisional realignment. This has changed the names of the Plans and Policy Branch to Policy and Rulemaking, the Risk Analysis and Data Branch to Information Technology, the Operations Support Branch to Mission Support, and Inspections & Enforcement Branch to Field Operations. Figure 2 reflects those changes; however, in this report we reference the branch names that were in use during our fieldwork.

Chemical Security Inspectors within the Inspections & Enforcement Branch are the primary representatives of ISCD to the regulated community and the Chemical Sector. They are responsible for managing, coordinating, and



conducting inspections, compliance assistance, and outreach activities. Chemical Security Inspectors are located in 10 regional areas within three districts across the Nation, and interact with 4,403 regulated and numerous unregulated facilities. Appendix D shows the ISCD regional locations, number of field staff, and CFATS-regulated facilities as of October 2012.

CFATS Program Budget

ISCD has received almost \$443 million to develop and implement the CFATS Program and Ammonium Nitrate Security Program.⁷ These funds have been used for personnel, training, travel, information technology systems, and equipment, among other things. Table 2 shows the CFATS budget by fiscal year.

Table 2: CFATS Budget by Fiscal Year

Fiscal Year	Personnel Costs	Training, Systems, Program Support	Total Funding
2007	\$0	\$22,000,000	\$22,000,000
2008	5,632,000	44,368,000	50,000,000
2009	11,219,000	66,781,000	78,000,000
2010	33,495,000	69,868,000	103,363,000
2011	33,428,000	62,502,000	95,930,000
2012	32,965,000	60,383,000	93,348,000
Total	\$116,739,000	\$325,902,000	\$442,641,000

Source: ISCD budget data.

Challenges Implementing CFATS and Internal Reviews of ISCD

ISCD has experienced significant challenges in implementing the CFATS Program, such as high turnover among senior leadership, numerous organizational realignments, shifting mission focus, and a large increase in human capital resources without appropriate office facilities. As a result, in 2011 NPPD's Under Secretary and IP leadership requested that the NPPD Office of Compliance and Security (OCS) conduct an inspection of ISCD. OCS is responsible for factfinding inquiries regarding misconduct allegations within NPPD. OCS' inspection was conducted from April to September 2011, and highlighted a number of deficiencies within ISCD functional areas, including fleet management, purchase card administration, travel management, property management, human resources/performance management, and facilities planning.

⁷ Section 563 of the *FY 2008 DHS Appropriations Act*, Public Law 110-161, authorizes DHS to "regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility...to prevent the misappropriation or use of ammonium nitrate in an act of terrorism."



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In July 2011, NPPD's Under Secretary requested newly hired ISCD leadership to review the division and the CFATS Program because of continued programmatic concerns. In November 2011, ISCD leadership provided the results of its review to the Under Secretary in an internal limited distribution memorandum. The memorandum identified three high programmatic priorities: approving SSPs; preparing for compliance inspections; and developing and implementing RBPS-12, Personnel Surety, and the Ammonium Nitrate Security Program.

In addition, the memorandum identified challenges having the greatest affect on the program's progress: inadequate training capability; overreliance on external experts for mission-essential tasks; no transition plan for new hires; no long-term or permanent program authorization; and the introduction of a union prior to the program's full establishment and maturation. As a result of the review findings, a corrective action plan was drafted with items relating to team, mission, and administrative issues. This action plan included the findings from the OCS inspection. In December 2011, the internal memorandum was leaked to news media, and several media outlets published articles with direct quotes from the memorandum.

In response to congressional requests after the internal memorandum was leaked, we assessed ISCD's efforts to implement the CFATS Program. Specifically, we reviewed whether: management controls are in place and operational to ensure that the CFATS Program was not mismanaged; NPPD and ISCD leadership misrepresented CFATS Program progress; and nonconforming opinions of CFATS Program personnel were suppressed or met with retaliation.

The scope of our review covers CFATS Program implementation from October 2006 through October 2012. After ISCD issued its November 2011 internal memorandum, program officials began efforts to complete items identified in the memorandum's action plan. Our review, however, did not focus on ISCD's efforts to address action plan items. Rather, at the request of Congress, the Government Accountability Office performed a review of ISCD's management and its progress to implement the action plan.

Many interviewees provided only general timeframes and frequently said that they could not recall the details of areas under review. Some interviewees' testimony was contrary to documents in official reports and email messages we received. In addition, some interviewees said they had documentation on specific events, but after we requested these documents, interviewees were frequently unable to provide requested information or provided insufficient information for a full analysis of issues raised.



Results of Review

As of October 2012, the CFATS Program has not yet been fully implemented, and concerns remain over whether it can achieve its mission, given the challenges the program continues to face. ISCD tried frequently to progress the program without fully addressing numerous issues, such as the CSAT tools and the SSP review process. A common explanation by program officials for the challenges is that CFATS is a new program. However, it has been more than 5 years since the program was created, almost \$443 million has been appropriated, and no facility has gone through the entire CFATS regulatory process.

Program progress has been slowed by inadequate CSAT tools, poorly executed processes, and insufficient feedback on chemical facility submissions. In addition, program oversight had been limited, and confusing terminology and absence of appropriate metrics led to misunderstandings of program progress. ISCD struggles with a reliance on contractors and the inability to provide employees with appropriate training. Overall program implementation efforts have resulted in a systematic noncompliance with sound Federal Government internal controls and fiscal stewardship, and employees perceive that their opinions have been suppressed or met with retaliation. Although we were unable to substantiate any claims of retaliation or suppression of nonconforming opinions, the ISCD work environment and culture cultivates this perception. Despite ISCD's challenges, the chemical industry views CFATS Program regulation as necessary to establish a level playing field across a diverse industry.

CFATS Program Tools Need Modification To Improve Efficiency, Effectiveness, and Utility

Most industry officials believe the CFATS regulation is sound and the performance-based philosophy is appropriate. However, ISCD needs to modify its CSAT tools to make them more efficient, effective, and easier to use. Currently, facilities enter information into the CSAT, but industry officials said results are of limited use.

SSP Tool Concerns Led Industry To Develop an ASP Template

ISCD initially solicited input from chemical industry representatives to develop the CFATS Interim Final Rule, RBPS, Top Screen, and SVA. Several industry representatives recalled an opportunity to test the Top Screen and to provide comments. However, when the SSP was developed, industry officials said that



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

they were not consulted. Industry officials are unsure of the reason but mentioned that ISCD changed contractors prior to SSP development.

According to industry officials, the SSP tool does not require facilities to provide all information necessary for ISCD to complete the SSP review process. The SSP tool is primarily a list of yes or no questions with some short answer questions. The tool also includes a number of text boxes that provide facilities with the option to include additional information. It is not a security plan and is of limited use to facilities. Many industry officials described filling out the SSP tool as time and resource intensive. Yes or no questions do not always allow facilities to account for unique site characteristics, such as a natural security barrier. For example, a facility may have fencing on three sides but a cliff on the fourth. ISCD officials assumed that industry would use the optional text boxes to expand upon its answers in the SSP to describe security measures. This assumption limited ISCD's ability to make an informed decision regarding a facility's capacity to meet the RBPS without physically observing the facility.

Industry officials raised additional concerns about redundancies in Top Screen, SVA, and SSP questions. They said ISCD should modify the CSAT to allow for prepopulation of data from the Top Screen, to the SVA and the SSP as applicable.

In contrast to the CFATS Program, industry representatives applauded some IP voluntary programs and recommended that these be used to assist the CFATS Program. For example, IP's Protective Security Advisor Program has a field cadre that specializes in public and private outreach and activities to reduce security risks of critical infrastructure and key resources across all sectors. In addition, many industry members use IP's Voluntary Chemical Assessment Tool, which allows owners/operators to identify current facility risk levels using an all-hazards approach and also facilitates a cost-benefit analysis. The Voluntary Chemical Assessment Tool has been adapted into some private industry security programs, and industry officials said it is a simple tool that could have easily been adapted for CFATS. However, since CFATS Program development, ISCD management has separated the IP voluntary and regulatory programs. This action impedes ISCD's ability to identify and apply best practices across programs.

Because both industry and ISCD experienced challenges with the SSP tool, industry representatives noted that other regulatory programs already accept ASPs as an alternative way to meet regulatory requirements. For example, while implementing the *Maritime Transportation Security Act*, the U.S. Coast Guard



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

(USCG) worked closely with industry to develop ASPs.⁸ This ASP process allows industry to develop one plan for several vessels of similar size and purpose, which cut the number of plans submitted from 10,000 to 3,000. This process saves industry and USCG resources, time, and funds, while also improving the relationship between the Federal Government and regulated industry.

ISCD is trying to address SSP tool concerns by working closely with the American Chemistry Council in support of its efforts to develop an ASP template. According to ISCD staff, as of July 2012 there are more than 425 ASPs queued to the CFATS Program out of approximately 4,000 total plans for review.

Most industry representatives we spoke with said they have submitted or plan to submit ASPs for their CFATS-regulated facilities. Although ISCD may not approve an ASP template, it can inform each facility whether its ASP is appropriate, and then industry can distribute an unofficial template. In the summer 2012, a chemical facility in Michigan conducted an ASP pilot. A similar test is pending at a facility in Indiana. ISCD is also discussing ASP templates with other trade associations, such as the Society of Chemical Manufacturers and Affiliates. ISCD leadership was unsure whether facilities will shift to the ASP, since ISCD plans to modify the SSP tool as well. ISCD officials said that they have had discussions with industry about all CFATS tools, including making each more intuitive, which should lead to an easier to use and more useful end product.

Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #1:

Modify Chemical Security Assessment Tools to capture facility data efficiently and ensure that the tools provide meaningful end products for industry users and ISCD.

⁸ The *Maritime Transportation Security Act of 2002* (P.L. 107-295) was enacted to ensure greater security for U.S. seaports.



Recommendation #2:

Document engagement with Office of Infrastructure Protection and DHS regulatory and voluntary programs to identify and implement existing tools and processes that can be leveraged to make Top Screen, Security Vulnerability Assessments, and the Site Security Plan tools more efficient, effective, and easier to use for the CFATS Program.

Management Comments and OIG Analysis

We evaluated NPPD's written response and have made changes to the report where we deemed appropriate. In their written response, NPPD said that our recommendations address areas already identified in ISCD's action plan. We, however, conducted an independent assessment of the CFATS Program. The report includes CFATS Program progress in multiple areas; much achieved as a result of ISCD's action plan. A summary of NPPD's written response to the report recommendations and our analysis of the response follows each recommendation. A copy of NPPD's response, in its entirety, is included as appendix C.

In addition, we received technical comments from NPPD and incorporated these comments into the report where appropriate. NPPD concurred with 19 recommendations, partially concurred with 1 recommendation and did not concur with 4 recommendations in the report. We appreciate NPPD's comments and contributions.

Management Response to Recommendation #1: NPPD officials concurred with Recommendation 1. In its response, NPPD said that improving the CSAT is one of ISCD's top priorities for FYs 2013 and 2014. In addition, input received to date from both the regulated community as well as internal ISCD users of the outputs of the CSAT applications, ISCD has identified a number of potential improvements that should help make all three of the primary CSAT applications—the Top-Screen, the SVA, and the SSP—more user-friendly, more efficient, and more effective.

Also to revalidate and formalize suggestions for improving CSAT and to identify any additional potential improvements, ISCD launched a "CSAT re-engineering and optimization" effort in 2012. ISCD is also soliciting input from members of the regulated community with which ISCD interacts on a regular basis and has scheduled three roundtables with members of the regulated community in various locations around the United States.



OIG Analysis: We consider NPPD’s actions responsive to Recommendation 1, which is resolved and open. This recommendation will remain open pending our receipt of documentation that the modified CSAT is implemented.

Management Response to Recommendation #2: NPPD concurred with Recommendation 2. In its response, NPPD said they agree that documenting engagement between DHS regulatory and voluntary programs to identify and, where appropriate, implement existing tools and processes that can be leveraged to make the CFATS Program more efficient and effective is a worthwhile goal, and they are committed to doing so. However, NPPD strongly disagree that the voluntary and regulatory programs have not previously collaborated and our claim that ISCD management has separated the IP voluntary and regulatory programs in a manner that impedes ISCD’s ability to identify and apply best practices for its program.

OIG Analysis: We consider NPPD’s actions responsive to Recommendation 2, which is resolved and open. This recommendation will remain open pending our receipt of dates, times, attendees, and meeting minutes for collaboration between voluntary and regulatory programs. In addition, NPPD should provide us documentation showing how this collaboration has resulted in leveraging pre-existing tools and processes for the CFATS Program.

SSP Review Process Has Hindered CFATS Program Progress

Despite ISCD receiving thousands of SSPs from facilities since July 2009, the first SSP was not approved until September 2012. Initial SSP submissions did not provide sufficient information for authorization and approval. In addition, ineffective communication within headquarters and with Chemical Security Inspectors complicated and delayed the review process. As a result, an SSP backlog developed, and ISCD staff perceived pressure to authorize and approve SSPs. ISCD leadership acknowledged the challenges with the SSP review process and established a working group to modify it.

Issues With SSP Quality and Ineffective Communication Within ISCD

During our fieldwork, the Federal Review Center (FRC) within ISCD’s Compliance Branch reviewed SSPs and ASPs. Three groups composed the FRC: chemical security, cyber security, and physical security. Once a facility submitted an SSP through the CSAT, Oak Ridge National Laboratory sent the SSP with a workbook to ISCD. The workbook contained a protective measure index for each RBPS, against which ISCD evaluated the SSP. ISCD established a scoring system for SSPs



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

that ranges from 1 to 100; SSPs receiving below a certain numeric threshold are considered “unfavorable.” When reviewing initial SSPs received, the FRC was unable to make any favorable determinations because of insufficient information in the SSPs.

To address poor SSP quality and unique site characteristics of facilities, ISCD created the Pre-Authorization Inspection in 2010. During this inspection, Chemical Security Inspectors visited facilities to inform owners/operators how to submit SSPs properly. ISCD employees said that the pre-authorization inspection improved subsequent SSP submissions, but many were still not adequate for authorization. While the CFATS Interim Final Rule does not require a Pre-Authorization Inspection, ISCD used it as a means to assist facilities improve the information and quality of their submissions. With this information, ISCD would be in a better position to move forward with authorizing SSPs. Many ISCD employees said that ISCD should have stopped the review process and revised the CSAT after identifying problems with SSPs, because ISCD could not authorize inadequate SSPs.

Another issue in the SSP review process was inefficient communication within ISCD and between ISCD and facilities. Although the FRC subject matter experts were tasked with reviewing facility SSPs, it was ISCD practice that the FRC not contact facilities directly. When there were questions concerning a facility’s SSP submission, direct communication with the facility was limited to headquarters compliance case managers and field Chemical Security Inspectors. As a result, some FRC officials used internet searches to find facility information, and then contacted the Chemical Security Inspectors when additional information was required.

Perceived Pressure To Approve SSPs

ISCD employees felt pressured to determine SSPs as favorable. SSPs that are determined unfavorable by the FRC are sent to a technical panel, the Quality Assurance Quality Control group, and then to the compliance case manager, and require a consultation with DHS’ Office of General Counsel (OGC) representatives to NPPD. ISCD employees described instances when the Quality Assurance Quality Control group returned unfavorable SSP determinations to the technical panel for additional review, which ISCD employees interpreted as pressure to overturn the determination and declare the SSP favorable. Quality Assurance Quality Control group members were not technical experts, and multiple ISCD employees questioned the documentation for overruling unfavorable determinations. ISCD employees thought it would be better to deem the SSP unfavorable during the FRC review than at a Chemical Security Inspector



Authorization Inspection. Informing facilities of SSP issues during the review process allows for corrections to be made prior to Authorization Inspections, which saves time and resources for both the industry and ISCD.

Leadership Acknowledged SSP Review Challenges and Proposed New Processes

When the Compliance Branch started receiving SSPs in July 2009, there were no formal policies or procedures, and only one official directed all subordinates and branch activities. Personality issues resulted in differences of opinion on how to review and authorize SSPs. For example, this same official thought every facility had to pass each RBPS metric, which was contrary to the CFATS regulation. As a result, ISCD used a metric-by-metric approach and was unable to authorize most SSPs received, which contributed to a backlog.

Addressing SSP Backlog

IP leadership said it was made aware of SSP review status and associated backlog challenges in June 2010; however, the extent of the backlog was not conveyed to them. Designing a long-term SSP review process became an action item on the November 2011 internal ISCD memorandum's action plan. ISCD established an SSP Working Group in March 2012 to develop a long-term review process that is consistent, defensible, and timely. The working group encountered challenges in analyzing the SSP review process since only a few SPPs had been authorized or conditionally authorized as of June 2012. Conditional authorization is a caveat created in 2011 to move SSPs forward by adding specific technical conditions that must be addressed during a Chemical Security Inspector facility Authorization Inspection.

The RBPS guidance for authorizing SSPs makes it difficult for reviewers to decide whether the level of security is appropriate at the tiered facility. As a result, the SSP Working Group replaced the metric-by-metric approach with a holistic approach in June 2012. Under the holistic approach, SSPs have to satisfy all applicable RBPS only to a degree commensurate with their assigned tier. The SSP Working Group drafted a report in June 2012, which proposed an SSP and ASP Long-Term Review Process.⁹ The report described the thousands of pending SSPs as a "tsunami headed right for a process that has been documented to be slow to mature and confusing to many of the active participants." In its analysis

⁹ This document analyzes ways and means to execute SSP review, authorization, and inspection as required by the CFATS regulation. The key objectives of this analysis were to (1) identify courses of action to achieve an effective and efficient long-term SSP and ASP review process; and (2) using the long-term process as a framework, provide near-term solutions to the current SSP review backlog.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

of the existing process, the SSP Working Group estimated that the rate of SSPs advancing to the authorization stage is less than 120 per year, requiring 70 years to complete all SSP reviews.

According to the June 2012 report, with existing field personnel and using an average of three Chemical Security Inspectors per inspection, ISCD would be able to complete 813 inspections per year. With the requested addition of 32 Chemical Security Inspectors in fiscal year (FY) 2014 and 32 more in FY 2015, the estimated date to complete the backlog would be FY 2018. However, these requests were not approved and the CFATS Program did not receive the additional inspectors.

Modifying SSP Review Process

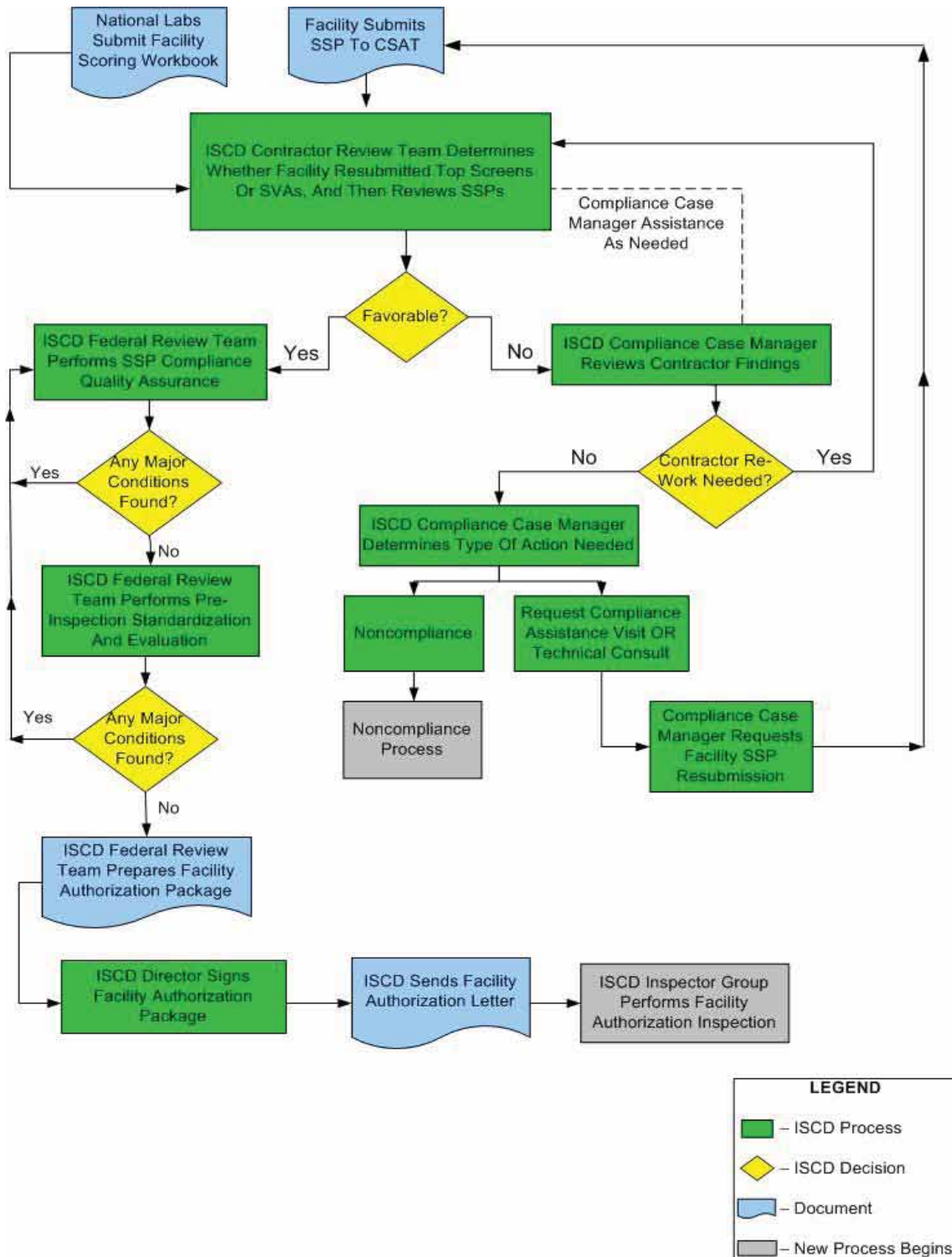
In June 2012, the SSP Working Group also proposed a new SSP review process to include a Standardization & Evaluation Group, which was described as a compilation of representatives from the technical panel, Quality Assurance Quality Control Group, policy, and Chemical Security Inspectors. Compliance case managers will guide facilities through the CFATS process from Top Screen to SSP final approval. ISCD leadership said that in the long term, ISCD will probably start assigning compliance case managers to the field to enhance working relationships. Figure 3 shows the steps of the SSP authorization process.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 3: SSP Authorization Process



Source: OIG Analysis of ISCD Data.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

To develop the new SSP review process, the SSP Working Group compared how regulatory programs at other departments and agencies, such as the Transportation Security Administration (TSA) and USCG, review and approve security plans. This review determined that most plans are generally approved at the regional level, with headquarters elements providing guidance, policy, and oversight. Most personnel are in the field, with only a small support staff at headquarters.

Several Chemical Security Inspectors said that SSP reviews should begin in the field to determine whether plans are sufficient for headquarters review. One field employee said that inspectors reviewing the SSPs would provide greater consistency, and inspectors could reduce the backlog because of the number of staff spread across 10 regions. As of October 2012, there were 114 Chemical Security Inspectors and nine support personnel dedicated to field operations. However, concerns about the consistent application of ISCD processes across field regions remain and undermine the viability of this option. In addition, the SSP Working Group determined that ISCD is not currently structured, and does not have established policies or Chemical Security Inspectors trained, to support decentralized program implementation.¹⁰

In addition, the June 2012 report recommended that a cross-training program be established within ISCD to facilitate integration of the two levels—headquarters to region and region to headquarters—to be based on personnel development requirements.¹¹ Several inspectors agreed that rotational assignments to the FRC would provide the FRC with the personnel and field perspective needed to review the SSPs.

As of October 15, 2012, ISCD has authorized or conditionally authorized 95 SSPs and conditionally approved 3 SSPs. Compliance Inspections for facilities with conditionally approved SSPs should begin in the fourth quarter of FY 2013. ISCD has begun to define processes and procedures for the Compliance Inspections and to train inspectors accordingly. ISCD leadership hopes to start conducting 40 Authorization Inspections per month in January 2013. ISCD continues to work on developing new procedures for SSP reviews and plans to have all Tier 1 and Tier 2 facilities approved by April or May 2014.

¹⁰ *SSP and ASP Long Term Process Review*, June 2012 Draft Report (FOUO), p. 28.

¹¹ *Ibid*, p. 31.



Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #3:

Provide evidence of how the revised long-term Site Security Plan review process has reduced the Site Security Plan backlog for all tiers.

Recommendation #4:

Define, develop, and implement processes and procedures for Compliance Inspections, and train CFATS personnel to conduct Compliance Inspections.

Management Comments and OIG Analysis

Management Response to Recommendation #3: NPPD officials concurred with Recommendation 3. In its response, NPPD said the updated SSP authorization, inspection, and approval rates currently occurring demonstrate that the updated SSP review process is reducing the SSP backlog for all tiers, beginning with Tiers 1 and 2. During the first half of 2012, ISCD clarified some of the policies regarding SSP reviews, finalized the development of a new SSP review process, trained SSP reviewers on the new process, developed a CFATS Inspections Standard Operating Procedure, and trained the entire CFATS Chemical Security Inspector Cadre on the new inspections procedures.

From October 2012 through January 2013, ISCD completed its review of all Tier 1 facility SSPs and authorized an average of 36 SSPs per month, with a high total of 47 authorizations in January 2013. ISCD is projecting authorizations to hold at this pace, with 40 to 50 authorizations expected each month for the remainder of the fiscal year. ISCD is projecting a steady increase in the number of approvals going forward, with 30 to 50 per month expected starting in March 2013. ISCD intends to continue to track and report on these statistics, and believes the statistics clearly demonstrate the revised SSP process and other improvements have dramatically increased SSP throughput and are reducing the SSP backlog.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 3, which is resolved and open. This recommendation will remain open pending our receipt of monthly statistics on the number of conditional authorizations, authorizations, and approvals for FY 2013. Each monthly report should include the total number of outstanding SSPs.



Management Response to Recommendation #4: NPPD officials concurred with Recommendation 4. In its response, NPPD said it agrees that it is imperative to ensure that processes and procedures for scheduling and performing all CFATS inspections, including Compliance Inspections, are well documented and that CFATS personnel who conduct inspections are trained on how to properly conduct inspections. To that end, ISCD has developed a Standard Operating Procedure for Inspections of CFATS Covered Facilities, which defines the different types of inspections conducted by ISCD, enumerates roles and responsibilities related to inspections, and details processes and standard operating procedures for pre-inspection, inspection, and post-inspection activities.

During the summer of 2012, all of ISCD's CFATS Inspectors participated in one of five, 2 week training sessions on the new ISCD Inspection protocols. NPPD officials said that many of the lessons taught during the 2 week sessions are equally applicable to Compliance Inspections. NPPD intends to provide additional training more specific to Compliance Inspections to all of its Chemical Security Inspectors prior to their beginning to conduct those inspections in September 2013.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 4, which is resolved and open. This recommendation will remain open pending our receipt of training materials and implementation schedules specific to Compliance Inspections.

Facility Submissions Are Not Processed Timely

According to the preamble to the CFATS Interim Final Rule, "DHS expects that it will complete its review of the Top Screen, SVA, and SSP within 60 days" after submission.¹² Table 3 shows an analysis of 619 Tier 1 and Tier 2 facility submissions and ISCD response time. DHS completed its review of less than 10 percent of the 619 facilities within the 60 day timeframe. In addition, some Tier 1 and 2 facilities have not had a Compliance Assistance Visit (CAV), Pre-Authorization Inspection, or Authorization Inspection since submitting SSPs to the CFATS Program in September 2009.

¹² *Chemical Facility Anti-Terrorism Standards; Interim Final Rule*, 72 FR 17704, April 9, 2007.



Table 3: ISCD Response Times to Facility Submissions

Type of Facility Submission	Average Time To Receive Tier Assignment	Longest Observed Time To Receive Tier Assignment
Initial Top Screen	4.8 months	12 months
Updated Top Screen	6.9 months	30 months
SVA	7.5 months	18 months

Source: OIG analysis.

Although ISCD has developed a new long-term process for reviewing SSPs, industry remains concerned about the time it takes to provide facilities with tier assignments. The data in table 3 represent only the 619 Tier 1 and 2 facilities; however, the CFATS Program must also regulate 3,784 Tier 3 and Tier 4 facilities. While ISCD officials said CFATS is primarily focused on Tier 1 and Tier 2 facilities, the program should be mindful that it must regulate facilities in all tiers for being high-risk.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #5:

Identify and implement a process to improve the timeliness of ISCD determinations for all facility submissions.

Management Comments and OIG Analysis

Management Response to Recommendation #5: NPPD officials concurred with Recommendation 5. In its response, NPPD said it recognizes that responding to facility submissions in a timely fashion is important for the credibility of the program and continues work to reduce response times.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 5, which is resolved and open. This recommendation will remain open pending our receipt of monthly reports on ISCD response times to facility submissions for FY 2013.



Facility Resubmissions and Requests for Redeterminations Are Not Addressed Properly or Timely

Some facilities change their use and quantities of certain COIs; material changes require resubmissions to ISCD. Facilities must resubmit a Top Screen when there are material changes to operations or sites, referred to in the CFATS regulation as material modifications, and changes in ownership.¹³ The regulation also requires resubmission of Top Screens, SVAs, and SSPs at 2- or 3-year intervals, depending on tier level. In addition, a facility may seek a redetermination of its tier level by filing a request with IP's Assistant Secretary. Because the chemical industry is dynamic, the CFATS Program should not employ static processes.

According to the CFATS regulation, facilities may request a redetermination, which ISCD should address within 45 days. Industry officials were submitting redetermination requests, but in many cases ISCD did not act or respond within the 45 days required. For example, in November 2010, an ISCD employee went to Oak Ridge National Laboratory to discuss redetermination requests and discovered hundreds of pending requests. After a review, ISCD identified a backlog of 656 requests that developed after several ISCD senior staff decided that facilities should not be allowed to "tier out" of the CFATS Program based on a redetermination. The prevailing mindset was that facilities would try to manipulate the CFATS process to circumvent regulation. ISCD senior staff continued to view these facilities as high risk despite changes in processes.

ISCD officials told ISCD staff that the CFATS Program was not built to address multiple requests from one facility. Therefore, when a facility submits its Top Screen, it is on one track throughout the CFATS process, since ISCD did not have the resources to open a second track. As a result, Chemical Security Inspectors visited facilities that were either abandoned, had been purchased by another company, or had removed the COI entirely. This occurred because ISCD was using determinations based on original facility submissions, some dating back to 2009, which was an inefficient use of time and resources for both industry and ISCD. Once staff in the Compliance Branch discovered the issue, they spent from Fall 2010 until Summer 2011 trying to clear the backlog. As of October 2012, the program was still experiencing a backlog.

¹³ *Chemical Facility Anti-Terrorism Standards; Interim Final Rule*, 72 FR 17702, April 9, 2007.



Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #6:

Develop a strategy and implement a plan to address facility resubmissions and requests for redetermination as prescribed in the CFATS regulation.

Management Comments and OIG Analysis

Management Response to Recommendation #6: NPPD officials concurred with Recommendation 6. In its response, NPPD said that ISCD has established draft procedures and policies for receiving, reviewing, and responding to facility resubmissions and requests for redetermination. ISCD also has provided guidance to facilities on how to properly request a redetermination and file a resubmission, established criteria for how to effectively process the requests, and determined appropriate review and analysis channels. Each request is reviewed to determine whether the resubmission significantly affects the facility's processes and chemicals, or only has minor impacts. This determination allows ISCD to identify the appropriate next steps involving the facility, which may include a CAV, new tiering determination, updated SVA, updated SSP, and/or other action.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 6, which is resolved and open. This recommendation will remain open pending our receipt of finalized standard operating procedures and policies for receiving, reviewing, and responding to facility resubmissions and requests for redetermination.

Management of the Personnel Surety Program Resulted in Premature Expenditure of Funds

RBPS-12, Personnel Surety, requires regulated facilities to perform background checks and ensure credentials for facility personnel, and for unescorted visitors with access to restricted areas or critical assets. This includes measures designed to (1) verify and validate identity; (2) check criminal history; (3) verify and validate legal authorization to work; and (4) identify people with terrorist ties. Regulated chemical facilities are required to address how they will comply with RBPS-12 in their SSP. However, identifying individuals with terrorist ties is an



inherently governmental function and requires the use of information in the Federal Government watchlist. The watchlist is sensitive but unclassified, and is unavailable to regulated chemical facilities. To allow for RBPS-12 compliance, NPPD is developing the Personnel Surety Program.

Personnel Surety Checks

Through the Personnel Surety Program, NPPD is proposing to conduct terrorist screening using information submitted by facilities about “affected individuals.”¹⁴ Once affected individuals are identified, regulated facilities will then submit the required information to NPPD through CSAT. Table 4 shows the information that facilities must submit.

Table 4: Personnel Surety Submission Data

Data Elements Submitted to CFATS	U.S. Persons	Non-U.S. Persons
Full Name	Required	
Date of Birth	Required	
Gender	Must provide Citizenship or Gender	Optional
Citizenship		Required
Passport Information and/or Alien Registration Number	N/A	Required
Aliases	Optional	
Place of Birth	Optional	
DHS Redress Number ¹⁵	Optional	

Source: May 2011 DHS Privacy Impact Assessment for Personnel Surety.

Once the information is submitted, NPPD sends the facility a verification of the submission. NPPD is then responsible for vetting affected individuals’ information against the Terrorist Screening Database (TSDB). The Terrorist Screening Center (TSC) maintains the TSDB, which contains “information about

¹⁴ The May 2011 DHS Privacy Impact Assessment for the Personnel Surety Program defines affected individuals as facility personnel and unescorted visitors with access to restricted areas or critical assets.

¹⁵ The Redress Control Number is the record identifier for people who apply for redress through DHS Traveler Redress Inquiry Program. This program is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs or crossing U.S. borders.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism....”¹⁶

The TSC is staffed with employees from the various Federal departments and agencies it supports. DHS components authorized to be assigned to the TSC include staff from USCG, TSA, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, U.S. Secret Service, and OGC. According to ISCD staff, TSC officials offered NPPD officials the opportunity to place a detailee in the TSC to conduct CFATS TSDB vetting at no cost. Despite this offer, ISCD decided to use TSA to conduct CFATS TSDB vetting. ISCD officials said one reason they decided to use TSA so that ISCD could ensure situational awareness when there is a positive match at a chemical facility. However, ISCD has no authority or ability to investigate a chemical terrorist threat, and it cannot identify individuals with terrorist ties without TSC information.

NPPD intends to leverage other DHS component TSDB vetting results on affected individuals by collecting information to verify that the affected individual is currently enrolled in a DHS program that also requires a TSDB check equivalent to the planned CFATS Personnel Surety Program. These DHS programs are—

- Transportation Worker Identification Credential (TWIC™)¹⁷
- Hazardous Material Endorsement¹⁸
- Trusted Traveler Programs, including
 - NEXUS¹⁹
 - Free and Secure Trade²⁰

¹⁶ Homeland Security Presidential Directive-6, *Integration and Use of Screening Information to Protect Against Terrorism* (September 16, 2003).

¹⁷ The TWIC™ program is a TSA and USCG initiative that provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of facilities and vessels regulated under the *Maritime Transportation Security Act*, and all USCG credentialed merchant mariners. To obtain a TWIC™, an individual must pass a TSA security threat assessment.

¹⁸ TSA conducts a security threat assessment for any driver seeking to obtain, renew, or transfer a hazardous materials endorsement on a State-issued commercial driver’s license.

¹⁹ The NEXUS program allows prescreened travelers expedited processing by U.S. and Canadian officials through dedicated processing lanes at designated northern border ports of entry, at NEXUS kiosks at Canadian Preclearance airports, and at marine reporting locations.

²⁰ The Free and Secure Trade program is a commercial clearance program for known low-risk shipments entering the United States from Canada or Mexico. This program allows for expedited processing of commercial carriers who have completed background checks and fulfill certain eligibility requirements.



- Secure Electronic Network for Travelers Rapid Inspection²¹

NPPD Is Paying TSA To Vet Names Although No Names Have Been Submitted

In April 2010, ISCD management conducted an analysis of alternatives and decided to use TSA's services for CFATS vetting capabilities. Since April 2010, even though the Personnel Surety Program is not in effect, NPPD has paid TSA more than \$7.7 million to conduct TSDB vetting. ISCD leadership said that funds are paid to TSA to establish and then maintain the vetting capability at TSA; cover an appropriate portion of the underlying vetting infrastructure costs at TSA; conduct some vetting; and provide future positive match support. Funds were provided prior to the CFATS Personnel Surety Program implementation so that TSA would have adequate time to establish the specific CFATS vetting capabilities, and be ready to support CFATS as soon as the Personnel Surety Program went live. NPPD also has an interagency agreement with U.S. Customs and Border Protection, which provided \$67,500 to verify that an affected individual is enrolled in one of the Trusted Traveler programs. Some ISCD staff said they wanted to identify alternate ways to conduct TSDB searches, but were prohibited from doing so. TSC officials offered NPPD officials the opportunity to place a detailee in the TSC to conduct CFATS TSDB vetting. However, the DHS Integrated Planning Guide FYs 2011-2015 directs DHS programs to use TSA's enterprise vetting service for all transportation/private sector programs, which would include the CFATS Program.

ISCD is still in the early stages of developing the Personnel Surety Program. In July 2011, ISCD submitted the program's Information Collection Request to the Office of Management and Budget for review and approval; however, ISCD withdrew its request in July 2012.²² ISCD leadership said thinking evolved on the Personnel Surety Program since the initial request and ISCD wanted to ensure that more vigorous conversation with stakeholders took place. As of October 2012, ISCD leadership said that they expect to resubmit the Information Collection Request to the Office of Management and Budget.

²¹ The Secure Electronic Network for Travelers Rapid Inspection provides expedited U.S. Customs and Border Protection processing to preapproved, low-risk travelers for travel between the United States and Mexico. Applicants undergo a thorough biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices.

²² An Information Collection Request is a set of documents that describe reporting, record keeping, survey, or other information collection requirements imposed on the public by DHS or any other Federal agency. Each request must be approved by the Office of Management and Budget before a collection begins.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #7:

Limit funding for Personnel Surety Program vetting until the Office of Management and Budget has approved the program's Information Collection Request.

Management Comments and OIG Analysis

Management Response to Recommendation #7: NPPD officials non-concurred with Recommendation 7. In its response, NPPD said they will continue to perform careful and deliberate analysis prior to the expenditure of any funds related to the CFATS Personnel Surety Program, and will only allocate funding when deemed appropriate given all relevant factors. The status of the Information Collection Request is simply one of those factors, albeit an important one. Consequently, the Department cannot concur with limiting funding to the Personnel Surety Program based solely on the status of the Information Collection Request without considering all of the other factors that go into the determination of how and when to fund the CFATS Personnel Surety Program.

OIG Analysis: Although NPPD did not concur, we consider NPPD's actions responsive to Recommendation 7, which remains resolved and open. This recommendation will remain open pending our receipt of documentation that the Office of Management and Budget has approved the Personnel Surety Program Information Collection Request and that ISCD has sent names to TSA for vetting.

Congress Provided ISCD Additional Chemical Security Regulatory Responsibility

Section 563 of the *FY 2008 DHS Appropriations Act*, Public Law 110-161, amends the *Homeland Security Act of 2002*, and authorizes DHS to "regulate the sale and transfer of ammonium nitrate by an ammonium nitrate facility...to prevent the misappropriation or use of ammonium nitrate in an act of terrorism." Congress directed NPPD to "provide a plan to implement this new provision, including an analysis of the resources required to do so, and a proposal for reallocating funding within the NPPD for doing so."



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Ammonium nitrate is a chemical that exists in multiple concentrations and physical forms, and each concentration or form may have different security implications. Ammonium nitrate is generally used as a fertilizer; however, it is widely used as an explosive particularly in mining operations. The Department is primarily concerned with its use as an explosive. When combined with fuel oil in the proper proportions it can create an explosive mixture. Ammonium nitrate explosive mixtures are regulated by the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and the Department of Transportation, which regulates explosives for the purpose of preventing incidents during transportation. Ammonium nitrate was used in the 1995 attack on the Alfred P. Murrah Federal Building in Oklahoma City, OK, and was one of the chemicals used in the May 2010 attempted Times Square bombing in New York, NY.

ISCD has been given responsibility to develop and implement the Ammonium Nitrate Program. The following categories are expected to be included in the program:

- Registration activities, including TSDB checks,
- Seller verification of purchaser's registration and identity,
- Record keeping,
- Reporting theft and loss of ammonium nitrate,
- Inspections and audits, and
- Civil penalties and adjudications.

As of October 2012, the Ammonium Nitrate Program is still in the rulemaking process. A small team within ISCD is developing the Ammonium Nitrate Program; however, they have determined it difficult to build the program without clear guidance. ISCD is moving forward with a dual-functioning inspector cadre and will be hiring up to 18 inspectors for the Ammonium Nitrate Program and cross-training them on the CFATS Program. The ultimate goal is to have the Ammonium Nitrate Program start in FY 2014.

Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:



Recommendation #8:

Develop an action plan and guidance for implementing the Ammonium Nitrate Program, which incorporates lessons learned from CFATS Program challenges.

Recommendation #9:

Develop and implement a curriculum and timeline for training inspectors to perform both Ammonium Nitrate and CFATS Program duties and responsibilities.

Management Comments and OIG Analysis

Management Response to Recommendation #8: NPPD officials concurred with Recommendation 8. In its response, NPPD said the Ammonium Nitrate Security Program is a proposed regulatory program, its development is guided in large part by the regulations and procedures set forth in the *Administrative Procedure Act*, the authorizing statute, and Office of Management and Budget guidance with respect to rulemaking activities. NPPD has been working within the parameters established by those items to develop a final rule, action plan, and guidance for implementing the final rule. NPPD/IP has recently assigned a member of the Senior Executive Service to oversee the development and implementation of the proposed Ammonium Nitrate Security Program.

Throughout the rulemaking and planning process, ISCD has been evaluating lessons learned from the CFATS Program and incorporating them into the development of the Ammonium Nitrate Security Program rulemaking activities and implementation planning. In particular, ISCD believes there are a number of programmatic similarities between the proposed Ammonium Nitrate Security Program and the proposed CFATS Personnel Surety Program. NPPD intends not only to apply lessons learned from CFATS Personnel Surety efforts to the Ammonium Nitrate Security Program, but also to take advantage of relationships, processes, information technology, and other aspects of the CFATS Personnel Surety Program to the maximum extent possible.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 8, which is resolved and open. This recommendation will remain open pending our receipt of an action plan with milestones for implementing the Ammonium Nitrate Security Program and its accompanying guidance.

Management Response to Recommendation #9: NPPD officials concurred with Recommendation 9. In its response, NPPD said that ISCD is committed to ensuring that all personnel receive and maintain the appropriate level and scope



of mission-specific training in support of CFATS and Ammonium Nitrate Security Program implementation. This includes training not only for inspectors, but also for those individuals performing compliance, policy, and other activities in support of CFATS. Training for these personnel will be developed and executed over the next 2 years in a prioritized manner that best ensures ISCD's ability to complete its mission.

In support of this effort, ISCD will develop, implement, update, and maintain training programs as required, using the Analysis, Design, Development, Implementation, and Evaluation model of Instructional System Design as the baseline framework. ISCD officials said this framework will ensure that any training content is instructionally sound and adheres to DHS and Federally approved technology standards and regulations.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 9, which is resolved and open. This recommendation will remain open pending our receipt of the training curriculum and implementation timelines.

Confusing Terminology and Absence of Appropriate Metrics Led to Misunderstandings of CFATS Program Progress

When Congress granted DHS the authority to regulate high-risk chemical facilities, it required that an interim final rule be issued within 6 months. While DHS met this deadline when it published the CFATS Interim Final Rule in 2007, there appeared to be confusion throughout ISCD about the 6-month requirement. Some ISCD employees interpreted the statute as a mandate to stand up and implement the CFATS Program within 6 months.

Misinterpretations of congressional intent may have put unnecessary pressure on ISCD to develop and implement the CFATS Program, resulting in poor management oversight and internal controls, personnel issues, and missed milestones.

ISCD Used Ambiguous Language To Describe CFATS Program Progress

Representing CFATS Program progress accurately is complicated because ISCD has used confusing terminology. For example, there are various interpretations within ISCD of what actually constitutes a chemical facility inspection. The introduction of Pre-Authorization Inspections in 2010 allowed ISCD to demonstrate results toward compliance, although the described objective of a Pre-Authorization Inspection is nearly identical to a CAV. Some ISCD employees view these as separate activities; in a CAV, inspectors learn about a facility during



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

a site visit, whereas a Pre-Authorization Inspection focuses more on inspectors fine-tuning an SSP during a site visit.

In several congressional briefings, ISCD officials counted the Pre-Authorization Inspection and CAV as separate activities, with Pre-Authorization Inspections under the inspections category and CAVs under enforcement. ISCD leadership identified this issue and stopped referring to these activities as Pre-Authorization Inspections and instead included them under the CAV terminology. However, the terms “pre-authorization” or “preliminary” inspection continue to be used by ISCD staff and in congressional briefings. While these activities are productive, none are required under the CFATS regulation and should not be used as a primary source for portraying program progress.

As shown in table 5, ISCD has completed 1,293 Authorization Inspections, Pre-Authorization Inspections, and CAVs. At most, these activities represent less than one-third of the total 4,403 CFATS-regulated facilities, because Chemical Security Inspectors performed CAVs and Pre-Authorization Inspections at some of the same facilities where they conducted Authorization Inspections.

Table 5: Inspections and Compliance Visits by Fiscal Year

Fiscal Year	Authorization Inspections	Pre-Authorization Inspections	Compliance Assistance Visits	Totals
2008	N/A	N/A	99	99
2009	N/A	N/A	90	90
2010	3	119	107	229
2011	6	61	534	601
2012	10	N/A	264	274
Totals	19	180	1,094	1,293

Source: ISCD, August 29, 2012.

Department officials testifying before Congress frequently used ambiguous terms when discussing CFATS Program progress. For example, in a congressional hearing on March 6, 2012, NPPD’s Under Secretary said that ISCD will “finish the site security plan reviews for the Tier 1 facilities in the next several months.” It is unclear, however, whether “reviews” refers to the processing and basic review of an SSP or the actual SSP authorization.²³ In addition, the terms “authorized,”

²³ U.S. House Committee on Homeland Security, Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies, *The Chemical Facility Antiterrorism Standards Program: Addressing its Challenges and Finding a Way Forward*, Hearing, March 6, 2012.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

“conditionally authorized,” and “approved” are sometimes used interchangeably during congressional testimony, which leads to even greater confusion.

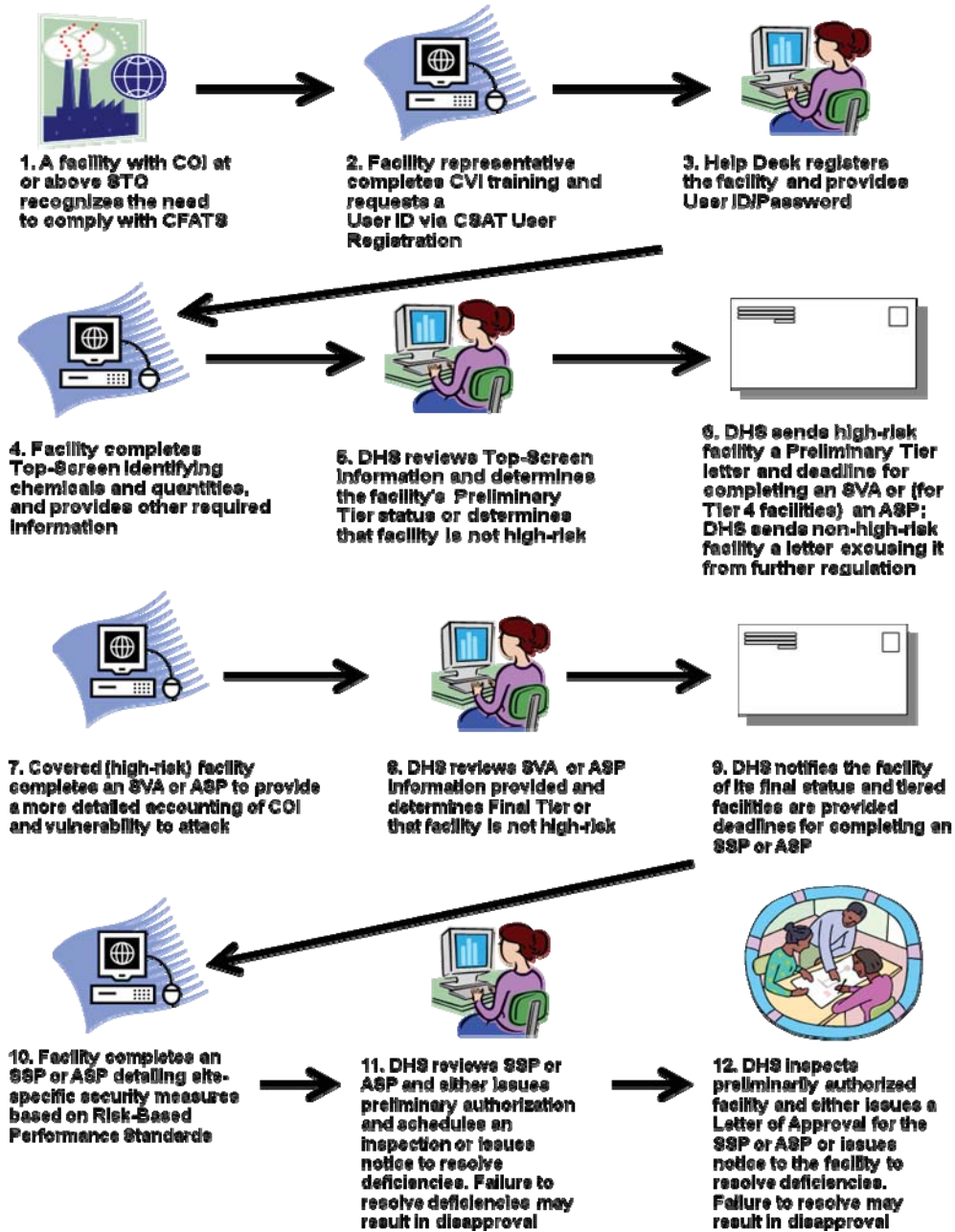
By simplifying the program into a 12-step process, Department officials also used confusing terminology that led to misunderstandings of CFATS Program progress. For example, during a hearing on March 6, 2012, NPPD’s Under Secretary testified that ISCD was in the 10th step of this process and said that NPPD “has come a long way from the beginning of the program.”²⁴ As shown in figure 4, Step 10 is the facility submission of an SSP and an ASP, which has been occurring since July 2009. In addition, Steps 1, 2, and 3 are administrative steps to initiate the CFATS process, and should not be counted toward program progress. This flowchart has been used in congressional briefings since 2010. Further, Steps 11 and 12 include multiple activities that could be broken down further, which would be consistent with how previous steps are presented. The flowchart does not explain what occurs following SSP approval or disapproval, and does not articulate the CFATS Program compliance cycle accurately.

²⁴ Ibid.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 4: ISCD CFATS 12 Step Process²⁵



Source: ISCD briefings to Congress.

²⁵ In Step 1, STQ refers to the Screening Threshold Quantity; there is a Screening Threshold Quantity for each COI, which when present at a facility requires the completion and submission of a Top Screen. In Step 2, CVI refers to Chemical-terrorism Vulnerability Information, which may reveal current vulnerabilities or other details of a chemical facility's security capabilities that could be exploited by terrorists. DHS sets rules for the protection of Chemical-terrorism Vulnerability Information.



ISCD Has Difficulty Measuring CFATS Program Performance

Initial CFATS Program milestones were the number of facilities covered under the regulation and how many Top Screen, SVA, and SSP submissions were received and reviewed. Due to limited inspection activities, the Department counts the number of facilities that have reduced or withdrawn the levels of COIs required for regulation under CFATS as proof of the program’s progress. While this is a positive occurrence, it is not the purpose of the CFATS Program. CFATS was created to ensure the security of facilities. Relying on “fewer regulated facilities” as a measure of success does not reflect the program’s added value in reducing risks at regulated facilities.

Projections for achieving CFATS Program milestones are not realistic. For example, in a 2011 response to Chairman Shimkus of the House Energy and Commerce, Subcommittee on Environment and the Economy, NPPD stated that the “Department is committed to meeting the goal of completing Tier 1 SSP reviews and issuing for each Tier 1 facility within calendar year 2011 either (1) a conditional authorization letter followed by the scheduling of an Authorization Inspection, or (2) a warning letter informing the facility that its SSP submission does not contain security measures that are adequate to meet applicable risk-based performance standards.” However, as of October 2012, these actions have not been completed, even though they have been communicated to Congress and were described in project management plans for the program.

Further, the majority of inspector activities consist of noninspection work, such as outreach to State and local emergency services, and facility meet and greets. As a result, it is challenging to measure the benefit of outreach and engagement activities. Table 6 shows facility outreach activities as provided by ISCD. While building relationships with industry and governmental partners is important, it is not an effective measure for determining progress in a regulatory program.

Table 6: Facility Outreach Activities by Fiscal Year

Fiscal Year	Meet/Greet	Presentations	Stakeholder Outreach	Total
2008	29	161	8	198
2009	136	147	no data	283
2010	385	102	1,634	2,121
2011	1,124	131	2,644	3,899
2012	2,310	116	1,604	4,030

Source: ISCD data.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

There is also the concern that inspector outreach activities are similar to those activities performed by IP's Protective Security Advisors.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #10:

Develop and implement program metrics that measure CFATS Program value accurately and demonstrate the extent to which risk has been reduced at regulated facilities.

Management Comments and OIG Analysis

Management Response to Recommendation #10: NPPD officials concurred with Recommendation 10. In its response, NPPD said that during FY 2012, the ISCD Program Management Office developed an Annual Operating Plan containing CFATS Program performance metrics for FY 2013 and beyond, including defined milestones, performance measures, and data points that will be tracked to monitor program performance. The performance metrics recognize both current and projected measurement start dates, as some business processes do not start until FY 2014 or later. These measures are subject to quarterly reviews and updates.

Additionally, ISCD recently updated its *Government Performance and Results Act of 1993* metric to reflect program progress better. Specifically, the CFATS Program developed a performance measure based on its RBPS with defined FY performance targets that measure the degree of covered facilities' compliance with the CFATS regulation. The new measure tracks and reports on the percentage of applicable RBPS that are confirmed through the SSP/ASP approval process as having been met by Tier 1 and Tier 2 covered facilities. Tier 3 and Tier 4 targets are planned to be defined in late FY 2013. This performance measure is reflective of the CFATS regulation's value and impact on regulated facilities' risk reduction. This measure has been approved as the reporting metric for the *Government Performance and Results Act* by both DHS leadership and the Office of Management and Budget.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 10, which is resolved and open. This recommendation will remain open pending our



OFFICE OF INSPECTOR GENERAL Department of Homeland Security

receipt of the ISCD Program Management Office Annual Operating Plan and updated *Government Performance and Results Act* metrics.

IP, NPPD, Congress, and DHS OIG Provided Limited Oversight of ISCD and the CFATS Program

Despite initial warning signs of challenges within ISCD, the CFATS Program was provided limited oversight to effect sound management practices and internal control. IP and NPPD leadership accepted updates from ISCD officials at face value, and in good faith that the CFATS Program was making progress. IP and NPPD officials responsible for briefing Congress on CFATS provided updates that reflected leadership's perception of program progress. This resulted in Congress applying less scrutiny over CFATS Program implementation.

It was not until late 2010, with the identification of an error in calculating field personnel pay, that a heightened level of oversight was necessary to address issues within ISCD. Although ISCD and IP officials reported several additional issues to DHS OIG, OIG referred the majority of those reports back to NPPD for review and investigation. When more CFATS Program challenges were made public in 2011 and 2012, Congress applied greater program scrutiny and oversight.

NPPD Oversight Was Limited During CFATS Program Development and Implementation

IP leadership was not always proactive about problems within ISCD, although a new regulatory program should have been a priority. ISCD employees said that former leadership was not actively engaged in managing ISCD, and there was limited situational awareness of daily activities.

In December 2009, the Office of Management and Budget requested NPPD to provide a report that described plans for full CFATS Program development and maturation. The May 2010 ISCD draft report said that the CFATS Program was not at final operational capability. However, ISCD was issuing final tier determinations, reviewing SSPs, and briefing Congress on initiating inspections. In addition, the report warned that excessive ISCD mission growth would hinder the proper execution of the CFATS Program. This report was never finalized or sent to the Office of Management and Budget.

In late 2010, an error in calculating Chemical Security Inspector pay was identified. In retrospect, the NPPD Under Secretary told us this was his "first



notion that the program wasn't all it was made up to be." Prior to that, the NPPD Under Secretary said that there had been some questions about the program not being where it should be—including questions about when the final tiering would be done. The pay issue led to an overall management review of ISCD, due to concerns that it was not the only problem. Between 2010 and 2012, multiple changes in ISCD leadership resulted in constant modification of the CFATS Program.

In 2012, IP and NPPD leadership received anonymous memoranda and emails from ISCD staff describing concerns with ISCD, such as unqualified staff and inaccurate tiering methodology. We were unable to determine actions taken to address the issues in those messages, but leadership expressed concern about where the documents originated. At a congressional hearing in March 2012, NPPD's Under Secretary expressed confidence in the new ISCD leadership's ability to manage the program. He added that NPPD has the clear intention to give ISCD leadership "full support—not that we didn't before, but we didn't realize how much support was necessary."²⁶

Previous IP leadership has not always trusted staff to report programmatic issues, as leadership did not always believe staff was providing all the necessary facts concerning CFATS Program progress.

Congress Applied Less Oversight Based on Information Conveyed by Department Officials

After establishing the CFATS Program, Congress was concerned with enhancing the program's mission by debating initiatives such as Inherently Safer Technology and Personnel Surety Program.²⁷ Members of Congress frequently said that they thought DHS has done a responsible job of establishing the CFATS Program. In its FY 2010 appropriations proceedings, Congress required monthly updates from ISCD on its hiring status and quarterly reports on the coordination of Federal chemical security efforts.

While a May 2011 letter from Chairman Shimkus to DHS about the CFATS Program did note that the pace at which SSPs for chemical facilities are reviewed and approved is a constant concern, it was not until after the internal ISCD

²⁶ U.S. House Committee on Homeland Security, Subcommittee on Cyber Security, Infrastructure Protection and Security Technologies, *The Chemical Facility Antiterrorism Standards Program: Addressing its Challenges and Finding a Way Forward*, Hearing, March 6, 2012.

²⁷ Inherently Safer Technology is a philosophy applied to the design and operation life cycle, including manufacture, transport, storage, use, and disposal to eliminate or reduce hazards to avoid or reduce the consequences of incidents.



memorandum leak that Congress heightened scrutiny and oversight. Some ISCD employees said they were glad that the internal memorandum was leaked, because it called attention to program issues and forced IP and NPPD leadership to address challenges.

Once Congress focused more attention on CFATS Program oversight, members began asking industry why it never reported these issues. However, a September 2011 American Chemistry Council survey of 139 representatives involved in managing more than 800 CFATS-covered facilities described industry concerns with the slow progress of CFATS implementation and the absence of clear guidance on tiering and compliance.²⁸ Despite concerns raised in the survey, most respondents supported the CFATS Program and its extension. Some industry representatives said that there needs to be more transparency through progress updates to the industry and Congress. We determined, however, that regular updates were provided, but did not convey CFATS Program challenges. Following the internal ISCD memorandum leak, industry representatives said that Congress became more interested in the money spent on ISCD vehicles and miscalculated inspector pay as raised in the leaked memorandum, rather than the steps and measures industry was taking to make chemical facilities more secure.

Congress Has Not Provided a Long-Term Authorization for the CFATS Program

Section 550 of the *Department of Homeland Security Appropriations Act of 2007*, Public Law 109-295, originally authorized DHS to regulate chemical security for 3 years. The 3-year authorization was set to expire at the end of FY 2009; however, the FY 2010 appropriations extended the authority by 1 year. This authority has been extended each year since FY 2010, despite calls for a long-term authorization from NPPD, industry, and members of Congress. The FY 2013 Continuing Resolution (H.J. Res. 117) provides ISCD's funding and authority to implement the CFATS Program through March 27, 2013. ISCD employees said that the absence of a permanent authorization causes additional uncertainty about job security.

Members in both chambers of Congress have proposed legislation that would extend the CFATS Program until 2018. In certain cases, proposed legislation expands and revises the CFATS Program as it currently exists. None of these bills have been passed into law as of October 2012.

²⁸ A Survey of CFATS Progress in Securing the Chemical Sector, American Chemistry Council, September 6, 2011.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Despite the challenges that DHS has had in implementing the CFATS Program, chemical industry representatives said that Congress should allow the program to mature rather than introduce new or revised statutory requirements. Industry representatives said that the extension of CFATS would bring some continuity to the process.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #11:

Develop a strategy and implement a plan to work with Congress and private industry to ensure long-term authorization for the CFATS Program.

Management Comments and OIG Analysis

Management Response to Recommendation #11: NPPD officials concurred with Recommendation 11. In its response, NPPD said the long-term authorization of CFATS remains a top priority for NPPD. Over the past few months, ISCD has worked closely with the DHS Office of Legislative Affairs to proactively engage Congress and reinforce the message that long-term authorization is a Departmental priority. The Department has advocated for long-term authorization in congressional testimony and has worked with its interagency partners to ensure that Congress receives a consistent message. Additionally, NPPD stands ready to provide whatever technical assistance or other input congressional members request in regards to CFATS reauthorization.

NPPD leadership believes there is nothing more critical to achieving long-term authorization of CFATS than the successful implementation of CFATS and recognition that the program is headed in the right direction. NPPD leadership is proactively sharing these success stories with members of Congress.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 11, which is resolved and open. This recommendation will remain open pending receipt of documentation showing continued congressional engagement regarding the long-term authorization for the CFATS Program.



DHS OIG Provided Limited Oversight of the CFATS Program

From 2008 to 2012, DHS OIG received several allegations regarding IP and ISCD employees and the CFATS Program. The allegations related to cronyism, misuse of Government equipment, unprofessional relationships, the leaked internal ISCD memorandum, and issues with contracts, ethics, and mismanagement. DHS OIG accepted one allegation for investigation and referred the other allegations to NPPD or DHS' Office of Management for investigation and action. Many of these investigations are still open and pending resolution.

Although DHS OIG's Office of Investigations determined that most of these allegations did not warrant its investigation, the number and severity of complaints should have prompted DHS OIG to initiate a review of CFATS Program activities. It was only after DHS OIG received multiple congressional requests that we initiated a program review.

The *Inspector General Act*, as amended, requires DHS OIG to keep both the DHS Secretary and Congress fully informed of problems and deficiencies relating to DHS programs and operations. OIG is responsible for conducting and supervising audits, inspections, and investigations related to DHS programs and operations. DHS Management Directive Number 0810.1 (MD 0810.1), *The Inspector General*, issued on June 10, 2004, requires DHS employees to report suspicions of violations of law or regulation to DHS OIG or the appropriate DHS operational elements.

According to MD 0810.1, allegations received by OIG can be retained or referred to DHS operational elements. Also, operational elements are required to transmit all allegations immediately upon receipt to OIG. The operational elements should not investigate allegations prior to OIG referral unless failure to do so would pose an imminent threat to human life, health or safety, or result in the irretrievable loss or destruction of critical evidence or witness testimony.

The DHS OIG Hotline is a resource for Federal employees and the public to report allegations of criminal and noncriminal activity associated with waste, abuse, or fraud affecting DHS programs and operations. DHS OIG's Office of Investigations maintains the hotline and processes complaints and allegations received for acceptance or referral. The DHS OIG Hotline received complaints from NPPD employees, but hotline staff could not provide us an accurate count of the complaints received. This is because DHS OIG's Office of Investigations uses a database that is name or case number driven, and it is not searchable by topic or beyond a DHS component level. To determine the number of complaints, we



met with hotline staff to query the database based on NPPD, IP, and ISCD employee and contractor names.

IP Leadership Efforts To Request DHS OIG Assistance

In December 2010, IP senior leadership drafted a letter to the DHS Inspector General requesting OIG assistance regarding potential deficiencies identified within ISCD. The potential deficiencies identified in the letter concerned Government vehicles, time and attendance, travel, equipment, and the ISCD internal management control processes. The letter requested OIG support in selecting a qualified contract audit company to perform an audit of ISCD. IP would fund the audit activities and designate a contact person to work with OIG to specify the tasks, scope of work, and deliverables.

IP senior leadership wanted concurrence from NPPD's Under Secretary before sending the request for assistance letter to the DHS Inspector General; however, the Under Secretary did not concur. The Under Secretary felt the areas were not criminal in nature and did not warrant OIG assistance. In discussion with the Under Secretary, he said it was part of NPPD's long-term strategic vision to establish an internal investigations program.

On April 14, 2011, the Under Secretary realigned the operational responsibilities for fact-finding and inquiry responsibilities within NPPD to its OCS. OCS' Compliance Investigations Division is responsible for providing fact-finding for NPPD programs and misconduct allegations, as listed in MD 0810.1, which DHS OIG declines to investigate. OCS would report directly to the Under Secretary and be staffed with personnel from NPPD's Federal Protective Service (FPS).

DHS OIG was contacted in June 2011 regarding the possibility that leadership did not disclose flawed tiering methodology when it was initially discovered. DHS OIG's Office of Special Investigations concluded that no formal investigation of the complaint was warranted, and forwarded the complaint to NPPD's OCS for whatever action was deemed appropriate. As of October 2012, the results of OCS' investigation were pending.

As of January 2013, DHS OIG is developing an internal review process to evaluate whether reported allegations should be referred to components for investigation and action or addressed by the OIG. This process will determine whether DHS OIG non-investigatory offices should conduct reviews of reported allegations prior to OIG referral to a component.



Overall Coordination, Communication, and Actions Taken To Address Facility Tiering Methodology Errors Were Ineffective, and Concerns Remain That Tiering Is Still Flawed

Several staff involved in CFATS development said that ISCD was under great pressure to begin tiering facilities. Therefore, the Top Screen and SVA tiering engines were created quickly, which left limited time for quality assurance and internal control. When an error was identified in December 2009 and January 2010 with the data used for final tiering, ISCD employees thought they had fixed the error in June 2010 and continued with facility tiering. In November 2010, ISCD staff identified an issue with the earlier approach taken to address the tiering error and reported these concerns to ISCD leadership in January 2011. This resulted in retiering facilities at all tier levels. However, as of October 2012, concerns remain that the tiering methodology is flawed. Appendix E provides a timeline of events surrounding the tiering methodology errors.

Tiering Engines Used by ISCD Contained Faulty Data

ISCD uses two tiering engines, one for Top Screen data that generates the preliminary tier and one for SVA data that generates the final tier. Argonne National Laboratory developed the original versions of these engines, which were later deployed in a classified information technology environment at Oak Ridge National Laboratory. The tiering engine algorithms are unclassified, but deaths and injuries calculated by these engines are classified. Some of the input factors are also classified, such as F1. The F1 Factor is used in tiering toxic COIs in both engines and also contributes to the tiering of sabotage COIs in the SVA engine.

Proxy data is used in the startup, development, and testing of a risk engine in an unclassified environment. Once the risk engine is ready for use, it is moved to a classified environment and proxy data is to be replaced with real data. The use of the unclassified environment accelerated risk engine development time. In December 2009, ISCD staff responsible for tiering said they observed anomalies in final facility tiering. However, it was in January 2010 that Oak Ridge National Laboratory determined that proxy data, not real data, was used in the F1 Factor final tiering and formally notified ISCD staff. ISCD told the laboratory to continue sending tier notification letters to facilities.

Starting in January 2010, ISCD staff held monthly tiering meetings. During the May 2010 meeting, ISCD leadership expressed concern with tiering results, which showed approximately 35 facilities potentially moving from a preliminary Tier 4 level to a final Tier 1 determination. Shortly after this meeting, a limited number



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

of ISCD staff discussed the F1 Factor issue, but did not immediately notify the acting ISCD Director. The acting ISCD Director relied on this group of subject matter experts and generally followed their advice on technical issues.

Initial Actions To Address F1 Factor Tiering Error

This group developed steps to address the F1 Factor problem. ISCD directed Oak Ridge National Laboratory to temporarily halt tiering activities and suspend distribution of the May 2010 facility tier notification letters. ISCD's Director notified IP leadership and NPPD staff of this action in a May 28, 2010, email message, as shown in appendix F. The IP's Assistant Secretary, Deputy Assistant Secretary, Chief of Staff, and Legislative Affairs, and NPPD's OGC and Principal Deputy Chief of Staff received the message.

ISCD officials decided that tier levels should not be revised for the estimated 3,800 facilities tiered before ISCD notified IP and NPPD leadership of the F1 Factor issue, even if the revised SVA risk engine would indicate a different tier result for those facilities. All facilities evaluated subsequent to May 31, 2010, would be tiered using the revised SVA risk engine. ISCD resumed distributing tier notification letters to facilities in June 2010. ISCD's Director provided IP leadership and NPPD staff with this update in a June 18, 2010 email, as shown in appendix F.

The F1 Factor Issue Was Raised Again and Resulted in Hundreds of Facility Tier Reassignments

In November 2010, while conducting a review of redetermination requests at the national laboratories, a new ISCD senior official noticed that many facilities experienced a tier change even though there was no change in the quantity of COIs. As a result, Chemical Security Inspectors were directed to suspend Pre-Authorization Inspections until ISCD assessed the tiering changes in early 2011. In December 2010, ISCD leadership changed, and staff provided briefings on their respective branches and activities. A Compliance Branch status paper discussed the F1 Factor tiering issue, and new ISCD leadership gave the paper to all ISCD senior staff for a response. Some senior staff were upset that the tiering error was brought up again and prepared a presentation to demonstrate that the F1 Factor issue had already been addressed. Another senior staff member said the presentation did not accurately convey the F1 Factor issue and suggested that ISCD leadership conduct further analysis.

As a result, ISCD leadership formed a group in February 2011, to work with the national laboratories and research the F1 Factor issue. Ultimately, ISCD retired



facilities that received tier determinations prior to May 2010. ISCD determined that 501 facilities were potentially affected. On June 27, 2011, ISCD distributed new tiering notification letters to the affected facilities.

Ineffective Coordination, Communication, and Actions Taken To Address the F1 Factor Issue

Several ISCD staff said that they wished they had more time and resources to conduct manual reviews of all tiering determinations. One staff member said that since re-tiering facilities affected by the F1 Factor, few SVA tiering letters have been distributed. Some ISCD staff said that it appeared that IP leadership was not concerned about the issue until rumors about media attention started. Then there was a push to fix the error, which some felt limited their ability to research and address the issue fully. The F1 Factor tiering error was not leaked to news media at this time; however, a June 30, 2011, internet chemical security blog posted that facilities were receiving re-tiering letters.

When IP leadership and NPPD staff were informed of the F1 Factor tiering error in June 2010, staff and leadership at all levels did not adequately report or take responsibility or corrective action. Communication to leadership within ISCD, IP, and NPPD in 2010 did not articulate clearly the severity of the F1 Factor tiering issue. Given the importance of final tiering determinations in the CFATS process, leadership should have requested further information. When the issue was presented again in June 2011, some IP and ISCD leaders denied receiving prior notification of the F1 Factor tiering error.

In retrospect, NPPD's Under Secretary told us that June 2011 was the first time he realized how badly managed CFATS was, because "by reading the emails, you would believe that the issue had been fixed, you would have to ask about the context to find out more...." and the Under Secretary "regrets that questions weren't asked at the time."

Additional Tiering Methodology Challenges Remain Concerning the V Factor

In February 2012, anonymous "concerned" ISCD staff notified Congress that there was an additional flaw in the risk engine methodology. The problem is called the V Factor. In structuring the tiering engine, ISCD did not have an appropriate way to reflect vulnerability in the risk equation for individual facilities. Risk is commonly defined as follows:

Threat x Vulnerability x Consequence = Risk.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In lieu of an acceptable option to reflect vulnerability, the CFATS Program set vulnerability at a constant for all facilities, regardless of tier. Mathematically, this makes vulnerability inconsequential in determining risk, because the CFATS methodology is labeling all regulated facilities as equally vulnerable, without considering the specific situation at each facility or security programs the facilities have in place. As a result, the risk engine is based only on Threat and Consequence, which is inconsistent with ISCD's intention of developing a risk-based program.

ISCD leadership said that while the V Factor is held as a constant in the risk engine equation, vulnerabilities are factored into the CFATS process, as facilities have to submit SVAs. However, because of the limited instructions provided in the SVA process, vulnerability assessment results were not considered valid. As a result, ISCD determined that it was not appropriate to allow vulnerability estimates to affect final tiering. ISCD leadership said although SVA vulnerability results are part of the CSAT data for each facility, the risk values used in the tiering analyses assumed that any facility could be attacked by an adversary and all would be equally vulnerable. This is why individual facilities were not assigned different vulnerability values.

ISCD leadership said that facilities have been retired, and ISCD has moved on from the F1 Factor issue. Following the F1 issue, ISCD implemented a three-phase plan: ISCD ensures that (1) the methodology is fully documented; (2) there is an internal review of the methodology; and (3) an external peer review takes place. The first and second phases of the plan uncovered some potential anomalies with approximately 20 toxic and inhalation chemicals, which may cause tiering changes for 34 facilities.

In September 2012, ISCD contracted with the Homeland Security and Studies Analysis Institute to perform the external peer review.²⁹ ISCD leadership expects a report with possible recommendations in spring 2013. ISCD leadership said that the external peer review may provide additional input on the Department's approach to vulnerability in the CFATS risk methodology.

²⁹ The Homeland Security Studies and Analysis Institute is a federally funded research and development center operated by Analytic Services Inc., on behalf of DHS. It delivers independent, objective analysis and specialized technical expertise.



Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #12:

Develop a methodology and reporting process to identify and address errors and anomalies that arise in the CFATS tiering methodology and risk engine.

Recommendation #13:

Provide the external peer review results, including comments on the V Factor, and ISCD's action plan to implement external peer review recommendations.

Management Comments and OIG Analysis

Management Response to Recommendation #12: NPPD officials concurred with Recommendation 12. In its response, NPPD said even though the anomalies occurred only with the tiering of sabotage and release chemicals of interest, which accounts for less than 15 percent of the CFATS regulated community, ISCD is undertaking a three-phased approach to review the tiering process. This three-phased approach, which is reflected in Action Item 94 of ISCD's current Action Plan, includes the following activities:

1. Thoroughly document all processes and procedures relating to the tiering methodology;
2. Conduct an internal DHS review of the complete tiering process; and
3. Conduct an external peer review of the risk-based tiering methodology.

The first two phases were completed by NPPD in 2012, during our review. The third item, the external peer review, began in January 2013. The peer review panel has been tasked with reviewing the existing CFATS risk methodology to see whether it is a justifiable and reasonable approach for tiering high risk chemical facilities. The results of the peer review are expected to be provided to the Department in the third quarter of FY 2013.

In addition to this formal review, the SVA and SSP review processes have been developed in a manner that requires multiple subject matter expert reviews of facility submissions. If at any point in time a subject matter expert identifies a potential anomaly in a facility's tiering, that anomaly is investigated to determine if it was a facility data error, an error within the tiering engine or risk



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

methodology, or not an anomaly at all. This supports a continuous improvement process, which ISCD has in place for all of its processes and methodologies.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 12, which is resolved and open. This recommendation will remain open pending our receipt of ISCD's process for investigating identified potential anomalies.

Management Response to Recommendation #13: NPPD officials partially concurred with Recommendation 13. In its response, NPPD said that ISCD supports the notion of acting appropriately on the external peer review findings and would be pleased to share those findings with appropriate entities.

OIG Analysis: Although NPPD partially concurred, we consider NPPD's actions responsive to Recommendation 13, which is resolved and open. This recommendation will remain open pending our receipt of the external peer review results and ISCD's plans to address the review's recommendations.

Pressure To Implement the CFATS Program Led ISCD To Rely on Contractor Support

In 2006, there were only a few Federal employees and several contractors in what would become ISCD. Some contractors were later converted to full-time Federal Government employees and served or continue to serve in leadership positions within IP and ISCD. Some ISCD employees were concerned that contractors were performing inherently governmental functions. They also said that some contractors were privy to critical program information and did not share it with colleagues once they were converted to Federal service.

Industry representatives were also concerned with the limited number of qualified chemical and physical security specialists within ISCD. Representatives said that ISCD became too reliant on contractors to develop the CFATS Program. For example, ISCD has contracts to handle the CFATS call center, support inspector operations, and provide policy, budget, and information technology assistance. In addition, multiple Department of Energy laboratories support the CFATS Program. Argonne National Laboratory has the technical engineering contract, Oak Ridge National Laboratory hosts and provides maintenance and operations of the CFATS information technology infrastructure, Sandia National Laboratory is used for economic modeling, and Idaho National Laboratory provides inspectors with cyber training.



Reliance on Contractors Contributed to F1 Factor Resolution Challenges

Dependence on contractors contributed to challenges when trying to diagnose and resolve the F1 Factor tiering error. IP dismissed the initial contracting firm that provided the factors for the Top Screen, because both could not come to a mutually acceptable agreement as to what mitigation actions were needed to avoid the potential for a conflict of interest. The documentation for the logic behind the tiering engine equations was not provided to ISCD when this contractor departed. The national laboratories supporting CFATS were unable to locate any direction or guidance related to creating and populating the classified environment for the SVA tiering engine. Further, ISCD subject matter experts reviewed submissions from the highest-tiered facilities, while contractors reviewed the lower-tiered facilities. However, current ISCD compliance employees said that the Federal employees and contractors are treated and assigned work equally.

Possible Conflict of Interest Between IP/ISCD Leadership and Contractors

ISCD's early reliance on contractors contributed to concerns regarding possible conflicts of interest and favoritism, which hinder proper contract selection and renewal. Several ISCD employees said that its contracts are not always awarded competitively. For example, in late 2010, the FRC contract to review SSPs was in the selection process. ISCD created a technical evaluation panel to review and award the FRC contract. Although three bidders were determined suitable, IP leadership instructed ISCD to suspend the contracting process, alleging that the technical evaluation panel was "corrupt." However, IP leadership should never have known the identities of personnel on the evaluation panel, nor the bidders.

Many interviewees with knowledge of the FRC contract said that the selection process was ultimately canceled in January 2011 due to concerns that multiple members of IP leadership had improper links to the bidders. However, ISCD leadership told employees that the division was "rescoping" and that no selection would be made on the FRC contract. Employees were concerned that no SSP reviews would be conducted for 1 year because the contract would have to start from the beginning of the contracting process. Despite the cancellation of the FRC contract award, ISCD has relied on separate contract services to provide subject matter expertise for SSP reviews since 2008.



A Perception Exists that Contractors May Be Performing Inherently Governmental Functions

Although we were unable to substantiate whether contractors were performing inherently government functions, a perception exists in ISCD. In addition, analysis of ISCD documentation demonstrates that contractors are performing closely associated governmental functions that have a high “direct impact” on ISCD’s critical mission.³⁰ ISCD does not always have the minimum percentage of Federal employees needed to perform or oversee these functions. In multiple ISCD branches, contractors outnumber Federal employees. For example, one employee estimated that contractors currently perform 70 percent of CFATS Program functions. Several ISCD officials said that much of the work is outsourced because contractors have been better performers and are more skilled in technical subject areas. Contractors also develop training material, and designed new training for the Chemical Security Inspectors.

Former ISCD leadership proposed an organizational realignment of ISCD in spring 2012, which it claimed would help reduce reliance on contractors, though a contractor assisted in developing the realignment. Multiple ISCD employees said ISCD should not have paid \$301,500 for contract support and should have explored whether IP or NPPD had internal resources to assist with the realignment.

ISCD intends to federalize more positions in the Compliance Branch, although contractors will still be used. However, we are concerned with the appearance that contractors may have been and are performing inherently governmental functions and closely associated governmental functions, as defined in the Federal Acquisition Regulation, Subpart 7.5 – Inherently Governmental Functions. Specifically, contractors appear to have performed the following functions listed in 7.503(c) Policy:

- (5) The determination of agency policy, such as determining the content and application of regulations, among other things, and
- (6) The determination of Federal program priorities for budget requests, and
- (7) The direction and control of Federal employees.

In addition, 7.503(d) provides examples of certain services and actions that are not considered to be inherently governmental functions. However, these

³⁰ DHS components are required to assess the degree to which accomplishing functions have a direct impact on the component’s critical mission(s), according to the October 31, 2011, DHS Balanced Workforce Strategy Guidance.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

services and actions may approach being in that category because of the nature of the function, the manner in which the contractor performs the contract, or the manner in which the Government administers contractor performance. Contractors appear to have performed the following functions in this category:

- (1) Services that involve or relate to budget preparation, including workload modeling, fact finding, efficiency studies, and should-cost analyses, etc.
- (2) Services that involve or relate to reorganization and planning activities.
- (3) Services that involve or relate to analyses, feasibility studies, and strategy options to be used by agency personnel in developing policy.
- (4) Services that involve or relate to the development of regulations...
- (6) Services in support of acquisition planning.
- (7) Contractors providing assistance in contract management (such as where the contractor might influence official evaluations of other contractors)...
- (9) Contractors providing assistance in the development of statements of work...
- (11) Contractors working in any situation that permits or might permit them to gain access to confidential business information and/or any other sensitive information (other than situations covered by the National Industrial Security Program described in Federal Acquisition Regulation 4.402(b)).
- (12) Contractors providing information regarding agency policies or regulations, such as attending conferences on behalf of an agency, conducting community relations campaigns, or conducting agency training courses.
- (13) Contractors participating in any situation where it might be assumed that they are agency employees or representatives...
- (18) Contractors providing legal advice and interpretations of regulations and statutes to Government officials.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #14:

Reduce overall ISCD reliance on contract personnel to avoid the appearance that contractors may be performing inherently governmental functions and closely associated governmental functions.



Management Comments and OIG Analysis

Management Response to Recommendation #14: NPPD non-concurred with Recommendation 14. In its response, NPPD said to ensure that ISCD has the appropriate mix of Federal and contractor skills, expertise, experience, and other assets necessary to effectively achieve the Department's mission, each new and recompeted contract is analyzed using the DHS Balanced Workforce Strategy tool to assess risk, ability to provide adequate oversight, and cost. Based on the analyses done to date, NPPD does not believe that ISCD is overly reliant on contract personnel, nor does NPPD believe that any contractors are performing inherently governmental functions or inappropriately performing closely associated governmental functions.

NPPD said that there is no substantiating evidence for any of the allegations made by us regarding contractors performing inherently governmental functions, or any specific examples of activities that give the perception of such prohibited activity. Nevertheless, ISCD, in conjunction with NPPD Finance, will perform an assessment of ISCD's current level of contract personnel to confirm that there is not an overreliance on contract personnel. Additionally, NPPD and ISCD will continue to review all new ISCD procurements under the DHS Balanced Workforce Strategy to ensure the Scopes of Work for contractors do not include any inherently governmental functions.

OIG Analysis: Although NPPD did not concur, we consider NPPD's actions responsive to Recommendation 14, which is resolved and open. This recommendation will remain open pending our receipt of ISCD's assessment of the current level of contract personnel.

ISCD Struggles To Provide Employees With Appropriate Training

When establishing the CFATS Program, ISCD leadership envisioned an academy to train Chemical Security Inspectors to enforce the CFATS regulation across regulated industry. However, this academy began training personnel before ISCD issued the CFATS Interim Final Rule, developed a program vision, or defined inspector roles and responsibilities. Recognizing the ineffectiveness of early training sessions, ISCD leadership developed a new inspections training course in June 2012. By focusing training efforts on Chemical Security Inspectors, ISCD has provided limited guidance to headquarters staff on responsibilities and career development. Most headquarters staff do not have formalized training, and frequently have to learn critical position duties and functions on the job with little guidance.



Chemical Security Academy Was Lengthy, Premature, and Provided Only a Basic Introduction

Legislation and departmental pressure gave IP officials the impression that CFATS was a fast-moving program. As a result, IP leadership accelerated inspector hiring and training before establishing a framework for the program. IP decided that the FPS inspector cadre would be a good resource for implementing the program quickly. FPS inspectors did not have regulatory enforcement experience or chemical experience, but did have physical security training. In March 2007, IP signed a memorandum of agreement with U.S. Immigration and Customs Enforcement to detail six Area Commanders and 30 GS-0080 Law Enforcement Security Officers (Inspectors) from FPS to provide full-time support to IP.³¹

The Chemical Security Academy was developed on the premise that a sustained, effective training program would ensure that inspectors and staff execute a uniform and fair enforcement of the CFATS regulation. The first Chemical Security Academy, referred to at the time as the Field Inspection Operations Training Program, began in February 2007 and had a curriculum that spanned 7 weeks. It consisted of 2 weeks of Hazardous Material Tech Training in Kansas City, MO; 4 weeks of coursework in Louisville, KY; and 1 week of site visits in Freeport, TX. The first three academies trained approximately 60 inspectors.

Former ISCD leadership believed that as inspectors were being trained, CFATS appendix A would be finalized, the Top Screen developed, and preliminary tier determinations made. However, SVA approval and appendix A finalization took longer than anticipated, and many interviewees said that ISCD leadership hired inspectors too soon. Additional materials and tools were integrated into academy trainings as developed and finalized. Overall, most inspectors thought the academy training provided a basic introduction to CFATS, but little or no insight into position duties or responsibilities, because the organization was developing. As a result, ISCD leadership stopped the Chemical Security Academy and stopped performing Authorization Inspections in July 2011. In addition, ISCD formed an inspector tools working group to conduct a review of all procedures, processes, and training for the inspector cadre.

The new training program started in June 2012, and ISCD resumed Authorization Inspections in July 2012. Overall, Chemical Security Inspectors said the new course was valuable because the CFATS Program is closer to full implementation.

³¹ In 2007, FPS was placed organizationally within U.S. Immigration and Customs Enforcement. In October 2009, FPS was transferred to NPPD.



However, some inspectors said it was a refresher course emphasizing consistency before Authorization Inspections were reinitiated and was a waste of time because it did not address the issues CFATS is experiencing.

ISCD Headquarters Does not Have Structured Training

Because it focused on training Chemical Security Inspectors, ISCD management did not develop structured employee training at headquarters. As a result, new employees often learn position roles and responsibilities on the job. For example, reviewing SSPs for authorization or approval is critical to the CFATS Program, but no structured training is provided for this review process. Although employees generally have Individual Development Plans, ISCD headquarters staff has limited opportunities for professional development due to funding constraints or a perception by management that employees are too busy to attend training.

Some staff said the inability to receive training has complicated their job performance and capabilities. Other employees expressed discomfort in performing duties assigned because of insufficient training. While field personnel are required to complete training prior to conducting a CAV or inspection, headquarters employees are not.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #15:

Develop and implement a learning curriculum that (1) describes position roles and responsibilities clearly; (2) provides comprehensive training plans to prepare employees to perform assigned duties; and (3) communicates measures to assess performance.

Management Comments and OIG Analysis

Management Response to Recommendation #15: NPPD officials concurred with Recommendation 15. In its response, NPPD said that in 2012, ISCD conducted human resources planning to determine and identify the human resources and the necessary skill sets required for program success. Based on these activities, ISCD realigned its organization on a functional basis and clarified functional unit roles and responsibilities. Using this and other information as a



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

baseline, ISCD is developing a Human Resource Plan which will include a staffing management plan and identification of training needs for all staff. ISCD is using a workforce analysis methodology to complete this Human Resources Plan. This workforce analysis will include:

- Conducting a job analysis for each position;
- Creating new/revised position descriptions and job/task analysis worksheets for each position;
- Identifying required skills and competencies for each job;
- Creating new performance plans and standards by job; and
- Implementing new Individual Developmental Training plans targeted at developing and/or maintaining required skills and competencies.

After completing the Human Resources Plan, ISCD intends to develop and disseminate an ISCD Employee Handbook that describes for all staff various aspects of the Human Resources Plan.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 15, which is resolved and open. This recommendation will remain open pending documentation that the ISCD Employee Handbook has been developed and disseminated to all ISCD employees.

Inability To Follow Sound Government Practices Has Resulted in Noncompliance and Wasted Resources

Since its inception in 2007, ISCD has struggled with applying sound Government practices to human capital issues, pay administration, and resource allocation. In addition, ISCD was often led by acting leadership, which complicates its ability to address these challenges. Time served in acting positions often exceeded allowable timeframes and was not always documented in employee personnel records. Some ISCD employees have moved into acting positions where they serve as supervisors without appropriate position descriptions, which complicates the performance review and rating process. ISCD field personnel were assigned to nonexistent regional offices and received incorrect locality pay and inappropriate Administratively Uncontrollable Overtime (AUO). ISCD purchased equipment and leased vehicles excessively. In addition, ISCD built open secret storage office space for its headquarters that was not needed.



ISCD Personnel Challenges Highlight the Need for Human Capital Changes

When the CFATS Program was established in 2007, DHS' Office of Human Capital handled all NPPD human resource issues. In November 2009, NPPD received delegated examining authority, which enabled it to hire personnel and make human capital decisions for ISCD and other offices within NPPD. In December 2009, NPPD created its Office of Human Capital. Employees from IP's Director of Management Office serve as liaisons to NPPD's Office of Human Capital and ISCD to facilitate human resource functions. Within ISCD, IP liaisons assist the Business Support Team to manage divisional human resource needs.

Although NPPD's Office of Human Capital is structured to encourage collaboration, human capital employees at all levels said ISCD leadership did not consult the Office of Human Capital as the authority for personnel issues, and that ISCD leadership refused to cooperate on human capital issues.

In addition, ISCD has not always notified NPPD's Office of Human Capital when personnel are placed in acting or detailed positions. According to Office of Personnel Management (OPM) regulations, a non-Senior Executive Service Federal employee may be temporarily detailed to a Senior Executive Service position in no more than 120-day increments. However, when the temporary detail exceeds 240 days, an agency must use competitive procedures for the individual to remain in the temporary position.³² Several ISCD acting Directors and Deputy Directors were in these positions more than 240 days without a competitive process, as shown in tables 7 and 8. Director C served in this position on three occasions, twice as acting and once as permanent Director.

³² 5 CFR § 317.903.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table 7: Chronology of ISCD Directors

ISCD Director	Dates
Director A	October 2006–March 2007
Director B (Acting)	March 2007–July 2008
Director C (Acting)	July 2008–November 2008
Director D	November 2008–November 2008
Director C (Acting)	November 2008–July 2009
Director C	July 2009–September 2009
Director E (Acting)	September 2009–December 2010
Director F (Acting)	December 2010–July 2011
Director G	July 2011–July 2012
Director H	July 2012–Present

Source: ISCD program data.

Table 8: Chronology of ISCD Deputy Directors

ISCD Deputy Director	Dates
Deputy Director A (Acting)	Date Unknown–November 2008
Deputy Director B	November 2008–November 2008
Deputy Director A (Acting)	November 2008–September 2009
Deputy Director C (Acting)	September 2009–June 2010
Deputy Director D (Acting)	June 2010–August 2010
Deputy Director C (Acting)	August 2010–December 2010
Deputy Director E (Acting)	December 2010–April 2011
VACANT	April 2011–July 2011
Deputy Director F	July 2011–July 2012
Deputy Director G (Acting)	July 2012–Present

Source: ISCD program data.

ISCD is not required to inform NPPD’s Office of Human Capital when appointing an acting supervisor for less than 120 days; as a result, Human Capital cannot maintain appropriate personnel records. For example, employees who have served in acting positions may not receive a Notice of Personnel Action (Standard Form 50), which is the official documentation of Federal employment and reflects appropriate credit for time served in positions. However, ISCD is required to notify NPPD’s Office of Human Capital when appointing an acting supervisor for more than 120 days.

When an employee is on a detail assignment, the employee’s position is still considered permanently occupied. The detailed employee cannot be officially replaced with a permanent employee. NPPD’s Office of Human Capital officials said that a valid, classified position description must be used to officially document temporary personnel actions such as details or temporary



promotions. NPPD's Office of Human Capital does not have written policy requiring acting supervisors to have a supervisory position description. ISCD personnel in acting supervisory positions said they have either not had supervisory position descriptions or have gone for significant periods of time without one, receiving the documentation only after numerous requests.

Acting Management Has Hindered ISCD's Ability To Evaluate Employee Performance Effectively

ISCD acting management has not provided sufficient monitoring of employee performance. NPPD's Human Resources General Instruction Guide, Performance Management Program for Non-Senior Executive Service Employees, establishes employee appraisal procedures. An appraisal is the process used to review and evaluate employee performance. Supervisors must monitor employee performance against performance expectations and apprise employees of their performance. Progress reviews are also required to be conducted and documented at approximately the midpoint in the rating cycle. NPPD's guide also requires that supervisors complete ratings of record within 30 days after the appraisal period concludes.

In addition, an interim rating should be prepared whenever an employee's supervisor leaves before the last 90 days of the rating period. When this occurs, the current supervisor should consider any interim rating when preparing the employee's annual rating of record. However, documentation we received demonstrates that not all employees received interim ratings. NPPD's guide also states that when a supervisor has not supervised an employee for a period of time to provide sufficient familiarity with the employee's performance, the rating period may be extended up to 90 days. However, rating documentation provided did not include any requests for extension, even though some acting supervisors said they do not have enough interaction with employees to conduct performance reviews and the rating process properly.

Further, NPPD's guide states that employees have the option to provide written self-assessments of performance. Some ISCD employees said they wrote their own performance reviews, which were then approved by acting supervisors with few or no changes.

Recommendations

We recommend that the Director of NPPD's Office of Human Capital:



Recommendation #16:

Develop NPPD-wide policy regarding appointment of acting management in accordance with Office of Personnel Management guidelines.

Recommendation #17:

Ensure that all employees serving in an acting supervisory capacity have a supervisory position description in accordance with Office of Personnel Management requirements.

Recommendation #18:

Ensure that all employees receive performance reviews according to NPPD's General Instruction Guide on performance management.

Management Comments and OIG Analysis

Management Response to Recommendation #16: NPPD officials concurred with Recommendation 16. In its response, NPPD said it has already developed and issued an NPPD Merit Promotion Plan that states requirements for details and temporary promotions that are consistent with OPM requirements. To ensure that NPPD managers and human capital staff at all levels of NPPD understand the policies surrounding the appointment of acting management, NPPD Human Capital intends to provide training on the topic to appropriate individuals.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 16, which is resolved and open. This recommendation will remain open pending receipt of the NPPD Merit Promotion Plan and training curriculum for appropriate individuals.

Management Response to Recommendation #17: NPPD officials non-concurred with Recommendation 17. In its response, NPPD said the term "acting" does not have a formal definition under OPM guidelines, nor does OPM require that employees performing supervisory duties in an acting capacity always have a supervisory position description. The term acting may be used to cover anything from full assumption position duties, to temporarily covering 1 day absences, to serving as a point-of-contact but not covering all aspects of the position. However, it is important that managers are diligent in applying the rules for details when temporarily assigning employees to other duties. To alleviate any



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

misunderstanding, NPPD is exploring developing Human Resources training for managers that specifically address these topics.

OIG Analysis: Although NPPD did not concur, we consider NPPD's actions responsive to Recommendation 17, which is resolved and open. The number of persons in acting supervisory positions and the duration of these assignments in ISCD frequently went against the intent of OPM guidelines. This recommendation will remain open pending our receipt of documentation that ISCD leadership positions are filled with permanent, qualified individuals and receipt of the Human Resources training curriculum to address rules for temporarily assigning employees to other duties.

Management Response to Recommendation #18: NPPD officials concurred with Recommendation 18. In its response, NPPD said that on December 31, 2012, NPPD's Employee and Labor Relations Office issued a memorandum on Performance Management guidance that requires all non-Senior Executive Service employees to receive at least one formal documented progress review throughout the performance cycle. A signed acknowledgement form, to include feedback from the supervisor, is to be provided to the employee. This memorandum also addressed a new requirement for the subcomponent Chiefs of Staff to document and validates dates each employee signed a progress review by using the NPPD Performance Plan and Appraisal Report Certification. This report is to be submitted to NPPD for progress reviews by March 15, 2013, and close-out reviews with summary ratings by August 9, 2013. Due to the new requirements implemented by NPPD, ISCD is on track to ensure all employees receive both a midyear and a closeout review, which will ensure that supervisors actively engage with employees on their progress throughout the performance cycle. Going forward, ISCD intends to use the Performance Plan and Appraisal Report Certification to track ISCD's completion of all required performance reviews.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 18, which is resolved and open. This recommendation will remain open pending our receipt of the NPPD Performance Plan and Appraisal Report Certification and evidence that all ISCD employees receive progress and closeout reviews.

ISCD Leadership Assigned Field Personnel to Nonexistent Regional Offices and Provided Incorrect Locality Pay

Federal guidance for location-based pay entitlements, commonly referred to as locality pay, resides in 5 CFR § 531.601-611. Entitlement pay is based on an



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

employee's duty location or worksite and offsets the higher cost of living in some areas of the United States. For example, the cost of living in New York City, NY, is higher than in Buffalo, NY, so the Federal Government offers a salary supplement to employees. Federal employees working in Buffalo get a 16.98 percent supplement to their base salary, while employees in New York City get a 28.72 percent supplement.³³ According to 5 CFR § 531.605, an employee's duty location or worksite, as documented in the employee's Standard Form 50, should always be the place where the employee regularly performs work.

When ISCD hired permanent field personnel from August 2008 through November 2010, duty stations and locality pay adjustments were based on the planned location of 10 regional field offices. The regional offices were to be established in Seattle, WA; Los Angeles, CA; Denver, CO; Houston, TX; St. Louis, MO; Chicago, IL; Atlanta, GA; Philadelphia, PA; Mercer, NJ; and Boston, MA. A regional office in Washington, DC, was added but later dropped. Locations were selected because of proximity to a large number of chemical facilities regulated by CFATS. Appendix D shows the number of regulated facilities by region. As of October 2012, ISCD has temporary offices in Houston, TX, and Philadelphia, PA, and a permanent office in Los Angeles, CA. Additional expansion to planned regional offices has been put on hold indefinitely by NPPD's Under Secretary to identify opportunities to consolidate field locations.

Acting ISCD Leadership Assigned Locality Pay Improperly

Because field office employees were hired before regional offices were established, ISCD leadership allowed inspectors to work from home under a Flexible Work Environment Standard Operating Procedure, which was signed by the acting ISCD Director in October 2008. We were unable to determine whether the acting ISCD Director coordinated with NPPD OGC officials or DHS Office of Human Capital before issuing this procedure. Under the procedure, a Chemical Security Inspector living in Tulsa, OK, could be assigned a duty location in the Houston, TX, regional office. As the regional office in Houston did not yet exist, the employee would be allowed to work from home in Tulsa. The employee's duty location remained Houston for pay purposes, although the work was not regularly performed in Houston. Tulsa is approximately 500 miles from Houston and has a lower cost of living. If an employee who lives in Tulsa was hired at a base salary of \$71,674, the Houston locality pay adjustment of 28.72 percent would raise the salary to \$92,259.³⁴ The locality pay adjustment for Tulsa is 14.16 percent, meaning that the employee should receive \$81,823.

³³ OPM 2012 General Schedule Locality Pay Table.

³⁴ OPM 2012 General Schedule Locality Pay Table, based on General Schedule-13, Step 1.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

As a result of the incorrect locality area assignment, the employee would receive \$10,436 more per year.

Job offer letters sent to field office personnel did not differentiate between base salary and locality pay adjustment; letters listed only the General Schedule (GS) grade with step and total salary. During the hiring process, several inspectors recognized that they were being offered the incorrect locality pay and contacted NPPD's Office of Human Capital and ISCD leadership to question the salary in the job offer letter. NPPD's Office of Human Capital representatives repeatedly told them that the locality pay offered in the letters was correct.

NPPD, IP, and ISCD Efforts To Resolve Incorrect Locality Pay

In February 2010, ISCD leadership began learning about improper locality pay assignments when several Chemical Security Inspectors complained about owing taxes to States in which they did not live. In July 2010, ISCD leadership went to NPPD's Chief of Staff, DHS' OGC, and Office of Human Capital for assistance with determining an action plan. After these consultations, ISCD leadership decided to change the duty location to the employee's residence to reflect where the employee was regularly working. On July 21, 2010, NPPD's Director for Resource Administration sent an email message to all ISCD field employees explaining the decision.

On September 29, 2010, IP's Assistant Secretary established an ISCD task force to review the locality pay issue. The task force studied inspector records to identify where each lived, traveled, and performed the majority of work; it determined that OPM guidelines do not set a definitive threshold that must be met for an employee to receive a particular locality pay. The only statement in the guidelines is that employees are entitled to locality pay in the area where the employee "regularly performs work."³⁵ In a 2011 memorandum to NPPD's Under Secretary, ISCD defined regularly worked as having spent at least 10 percent of nontravel, nonleave workdays in the employee's assigned locality. Employees who met this threshold were not overpaid and therefore would not have to repay the Federal Government.

The task force results divided the field personnel into three groups: those not affected because locality was assigned correctly; those who met the definition of regularly working and did not owe overpayment; and those who did not meet this definition and owed overpayment. Of the 117 Chemical Security Inspectors in FY 2010, 43 did not reside within assigned locality pay areas. However, 21 of

³⁵ 5 CFR § 531.605.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

these employees met the definition of having regularly worked in the assigned locality pay area, and 22 did not meet this definition. In November 2010, ISCD officially changed all field personnel duty stations to reflect home addresses and corrected locality pay where necessary.

Overpayments were calculated from the time the employee entered on duty until the overpayment ceased. Most employees were notified of the potential overpayment in NPPD's Director for Resource Administration July 21, 2010, email message. The July 21, 2010, email message date was then used in determining the period for which those employees' debt would be waived. The National Finance Center manages Federal employee debt collection for NPPD. On December 2011, the center sent official notification of overpayment to affected employees, as well as an explanation of employee rights concerning salary offset repayment agreements, rights to a hearing, and the waiver request process. As of October 2012, 22 employees have been determined overpaid, for a total of \$143,760.40.

ISCD field employees were frustrated at not obtaining clear, straightforward answers from NPPD's Office of Human Capital concerning the locality pay issue and resulting overpayments, which negatively affected field employee morale. Chemical Security Inspectors said the locality pay issue was a major factor in the decision to unionize in March 2011.

Unionization In Part as a Result of Locality Pay Issues

Chemical Security Inspectors chose to unionize in part because of how NPPD's Office of Human Capital handled locality pay issues. It is also believed that ISCD detailees from FPS led efforts to unionize, as they were union members while at FPS.

Under the 2011 Master Agreement between NPPD and the American Federal Government Employees Union, ISCD Chemical Security Inspectors are represented by Local 918. An FPS employee leads Local 918, which has five IP vice presidents, one of whom is an ISCD employee. All Chemical Security Inspectors may have union representation, whether or not they pay dues. However, field leaders do not have union representation because they hold supervisory positions.

NPPD's Employee Labor and Relations Office handles most union interactions. When ISCD leadership determines it is operationally necessary to make a change in working conditions, it has an obligation to provide the union with an opportunity for pre-decisional involvement. Subsequently, once ISCD leadership



finalizes a draft of the new policy or process concerning these changes, it has an obligation to provide the union with notification and an opportunity to bargain the proposed change. The union may also meet with ISCD leadership regarding employee issues such as discipline, where both sides discuss potential personnel actions.

The ISCD internal memorandum leaked in December 2011 negatively portrayed the union's effect on the division. While this initially damaged the relationship between ISCD and the union, both have made efforts to improve interactions. For example, ISCD leadership meets with union representatives weekly to discuss ongoing personnel issues. Overall, ISCD leadership and the union's relationship is cooperative and has improved.

ISCD Has Used Administratively Uncontrollable Overtime Inappropriately

ISCD Chemical Security Inspectors receive the maximum AUO allowable by OPM regulations; however, we were unable to determine a definitive rationale for why inspectors receive AUO. AUO usage reviews were not conducted as required, and activities to support AUO receipt have not been performed. As a result, inspectors were inappropriately paid approximately \$2 million in AUO for FY 2012.

AUO is a form of premium pay used to compensate employees who occupy positions that require substantial amounts of irregular, unscheduled overtime work that cannot be controlled administratively and cannot be scheduled in advance of the workweek. AUO pay is calculated as a percentage of an employee's base pay and can range from 10 percent to 25 percent.³⁶ The rate of AUO authorized for a position is based on the average number of irregular or occasional overtime hours worked per week. Table 9 shows the number of hours required to receive the corresponding AUO percentage.

³⁶ 5 CFR § 550.151.



Table 9: Hours Required To Earn AUO

Hours Required per Week	AUO Percentage Earned
3.1–5	10%
5.1–7	15%
7.1–9	20%
9.1 or More	25%

Source: 5 CFR § 550.154.

Rationale for Awarding AUO to Field Personnel Could Not Be Determined

NPPD policy requires that a certifying official submit a Personnel Action Initiator form to the Office of Human Capital to initiate the payment of AUO. The request must include a certification that work assigned to the employee is expected to meet the requirements for AUO premium pay, and that the position to which the employee is assigned is approved for AUO premium pay. NPPD Office of Human Capital and ISCD leadership were unable to provide us with documentation of AUO authorization for ISCD.

Former ISCD officials said that AUO was provided to Chemical Security Inspectors initially because of the anticipated accelerated CFATS Program implementation. The original job announcements for field personnel posted in August 2008 included the potential authorization of AUO, and offer letters stated that inspectors would be eligible for an AUO differential of 25 percent. A former ISCD leadership official said that AUO should have been made available, but not paid until inspection activities began, and should have started at 10 percent and progressed to 25 percent as necessary. Instead, ISCD inspectors were offered the maximum AUO before roles and responsibilities were defined or workload warranted the extra pay.

AUO Reviews Were Not Conducted as Required

NPPD’s OCS began an AUO audit in April 2011 as part of its larger ISCD inspection. After OCS determined that there were irregularities with AUO reporting, it decided that AUO needed a more in-depth review, because each NPPD office with employees receiving AUO managed it differently.

According to OPM regulations, a Federal agency providing AUO must review the percentage and verify that it matches the number of hours worked “at appropriate intervals.” OPM recommends that these reviews occur every 3 to 6



months. When the result of an AUO review demonstrates that an employee is not completing required hours of irregular overtime, the rate of AUO should be adjusted or, if appropriate, discontinued.³⁷ NPPD's AUO Policy, dated September 4, 2012, requires that all certifying officials review the time and attendance and related records for all employees receiving AUO premium pay to ensure that employees meet payment requirements for rates authorized. According to the policy, periodic reviews are to take place in January, April, July, and October each year.

ISCD's AUO Policy Was Applied Inconsistently

As there was no formal NPPD AUO policy until September 2012, ISCD's January 2009 AUO policy was an adaptation of U.S. Immigration and Customs Enforcement policy. ISCD's policy does not define qualifying tasks clearly, leaving AUO policy implementation to regional commanders. Inspectors did not receive adequate training, which led to insufficient understanding of AUO requirements. Most AUO guidance came from branch chiefs or regional commanders in ad hoc emails. Some regions provided Chemical Security Inspectors with additional guidance on how to claim AUO hours, and provided examples for each AUO category as listed in Chemical Facility Management System.³⁸ However, this led to inconsistencies in how inspectors across the 10 regions report AUO.

Activities Conducted Do Not Support AUO Pay at the Maximum Percentage

AUO requires employees to recognize circumstances when they must remain on duty. These circumstances must be a definite, official, and special requirement of the position. An employee must remain on duty because of compelling reasons related to continuing position duties. The need to function outside normal duty hours must be so compelling that the employee's failure to do so would constitute negligence in performing such duties.³⁹ However, according to the categories in the Chemical Facility Management System, all inspector activities qualify for AUO hours.

Several ISCD employees questioned how Chemical Security Inspectors can justify claiming AUO for inspections that can be scheduled during normal business

³⁷ 5 CFR § 550.161(f).

³⁸ DHS established the Chemical Facility Management System as a tool to verify data submissions provided by industry to identify any areas of noncompliance. The Chemical Facility Management System extracts facility information from the CSAT. The system also supports inspection activities, including inspection schedules, assignments, plans, trip planning, disposition, and findings/options for consideration.

³⁹ 5 CFR Part 550.153.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

hours, and how inspectors were justifying AUO when no inspections were taking place. Supervisors told inspectors that they had to get the required hours of AUO or it would be cut. This practice led inspectors to claim AUO hours for work that does not meet OPM guidelines.

In June 2012, ISCD completed an internal audit of AUO. ISCD’s AUO audit team reviewed each Chemical Facility Management System AUO entry from January 2011 to March 2012. The audit determined that ISCD has not been reviewing AUO in accordance with OPM policy. In addition, hours of AUO claimed by inspectors did not match hours meeting AUO requirements. Table 10 shows that not all inspectors met the hourly requirements for 25 percent AUO they were paid. In addition, the table demonstrates the discrepancy between what employees reported and what actually qualifies as AUO.

Table 10: First Quarter FY 2012, Claimed AUO Hours and Qualifying AUO Hours

AUO Level	Number of Personnel Claiming Hours Toward AUO Level	Number of Personnel With Hours that Qualify for AUO Level
25%	24	4
20%	31	9
15%	23	26
10%	15	21
0%	22	55

Source: OIG analysis of ISCD AUO audit.

The average grade level of an ISCD Chemical Security Inspector is GS-13. In FY 2012, the base salary (excluding locality area adjustments) for a GS-13, Step 1, was \$71,674. A 25 percent AUO level of premium pay would therefore add \$17,918.50 to the base salary. Based on ISCD’s AUO audit results, of the 115 inspectors claiming AUO in the first quarter of FY 2012, only 4 qualified for 25 percent AUO. In addition, approximately 50 percent of field personnel did not meet hourly requirements for any AUO level. Assuming that all Chemical Security Inspectors receive 25 percent AUO, this would result in approximately \$2 million spent on AUO in FY 2012 for inspectors who did not meet these requirements.

One reason for the discrepancy between hours reported and AUO qualifying hours is confusion over what qualifies as AUO activity. AUO pay cannot be provided for work that has been regularly scheduled. Regularly scheduled work is defined as work that is scheduled in advance of an administrative workweek. Work performed in a supervised office environment that does not require



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

independent investigative or other administratively uncontrollable work should not be counted as AUO. For example, some inspectors temporarily working at headquarters still claimed AUO. Also, hours that are clerical, administrative in nature, or easily scheduled in advance should not be counted for AUO. The ISCD AUO audit determined that several inspectors claimed AUO for training. The audit report offered next steps for consideration, including the elimination of AUO. As of September 30, 2012, ISCD leadership was still considering options.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #19:

Eliminate the authorization and payment of Administratively Uncontrollable Overtime for all ISCD personnel.

Management Comments and OIG Analysis

Management Response to Recommendation #19: NPPD officials non-concurred with Recommendation 19. In its response, NPPD acknowledged that there previously were some issues related to the application and management of AUO within ISCD, these issues are being addressed. Moreover, based on the findings of an internal audit of the ISCD AUO program, there are legitimate justifications supporting the use of AUO by ISCD Chemical Security Inspectors. Based on that audit, ISCD leadership has determined that the more appropriate path regarding AUO for ISCD Chemical Security Inspectors is to continue to permit AUO in a manner that evolves consistently with AUO rules and regulations, and that is supported by greater oversight, increased training, documented policies and procedures, and greater management controls.

To ensure that all components within NPPD follow proper AUO protocols better, in September 2012 NPPD issued an NPPD AUO Instruction, which established policies and procedures for the approval, certification, and payment of AUO. That document requires all employees occupying positions that have been approved for AUO, as well as the supervisors of those employees, complete training on AUO regulations, policies, roles, and responsibilities. Under that policy, NPPD is in the process of conducting a review to ensure that all positions within NPPD for which AUO is currently being claimed are appropriate for AUO.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Additionally, ISCD has recently completed draft division-level AUO guidance to expand on the guidance provided by NPPD. This draft guidance will enumerate specific CFATS-related activities that are and are not AUO eligible and will describe and detail the frequency of both supervisory reviews and formal audits (i.e., Periodic Reviews). This draft guidance is anticipated to be completed and signed by ISCD leadership by the end of April 2013.

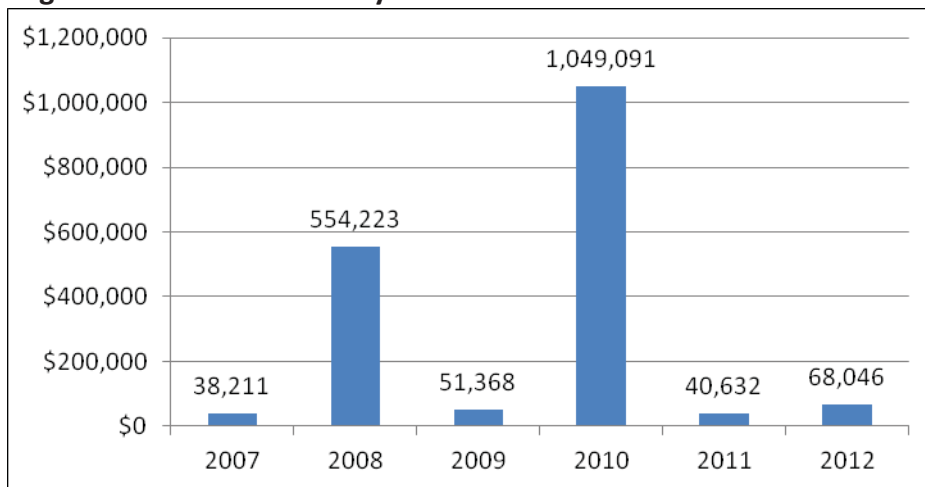
OIG Analysis: We consider NPPD's actions non-responsive to Recommendation 19, which is unresolved and open. AUO is a form of premium pay used to compensate employees who occupy positions that require substantial amounts of irregular, unscheduled overtime work that cannot be controlled administratively and cannot be scheduled in advance of the workweek. According to the Interim Final Rule, the Department will conduct audits and inspections at reasonable times and in a reasonable manner, providing covered facility owners and operators with advance notice before inspections, with limited exceptions. Therefore, inspectors schedule their work in advance, eliminating the need for AUO. This recommendation will remain open pending our receipt of documentation showing that AUO payments to inspectors are supported and justified by current and long-term activities.

ISCD Provided Unnecessary Equipment to Inspectors

ISCD officials identified and purchased equipment for Chemical Security Inspectors to perform inspection duties, and procured more than \$1.8 million in equipment, as shown in figure 5. However, CFATS Program progress was slow, and the roles and responsibilities of inspectors changed throughout implementation. As a result, ISCD later transferred approximately \$700,000 in equipment because it was unnecessary.



Figure 5: ISCD Purchases by Fiscal Year



Source: OIG analysis.

Initial purchase requests in FY 2007, FY 2008, and FY 2009 were for inspector equipment such as Toughbook™ laptop computers, docking stations, and global positioning system devices. Purchase justifications stated in part that field conditions include a wide range of weather and environmental elements. The equipment requested was to allow Chemical Security Inspectors to respond to critical situations and communicate with Federal Government entities, State and local law enforcement, and other team members and allow for the continuity of information technology capabilities.

ISCD ordered equipment to ensure that Chemical Security Inspectors would be equipped once hired and trained. According to an ISCD action memorandum to the IP Assistant Secretary in 2010, initial equipment requirements were based on ISCD staffing projections, as well as estimates of equipment replacement. Equipment projections were generally made 8 months prior to when the equipment was needed to account for the lengthy procurement timeline. This timeline includes market research and developing purchase requests for each item, approval by the ISCD Director, a bidding process, selecting a vendor, shipping, and receipt. As a result, and in part due to the pressure to implement the CFATS Program and the procurement timeline, ISCD ordered additional equipment before personnel were hired and trained.

CFATS Program Progress Was Slow, and the Roles and Responsibilities of Chemical Security Inspectors Changed

When FPS detailed inspectors to ISCD in 2007, the CFATS Interim Final Rule was still being written. According to several IP and ISCD officials, the CFATS mission



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

was not fully understood nor the inspectors' roles and responsibilities clearly defined. Initially, a first-responder role was envisioned. ISCD staff suggested that the concept of the first-responder role was a result of FPS' response activities after Hurricane Katrina in August 2005 and was incorporated into ISCD when FPS detailed personnel to the CFATS Program. This vision of inspectors as first responders resulted in ISCD ordering equipment such as hazardous material gear, spotlights, and rescue ropes.

ISCD's Excessive Purchases Resulted in Wasted Funds

When the procurement process was finished and purchased items delivered, ISCD leadership had changed, and the vision for CFATS had changed from a first-responder organization to regulatory enforcement. As items arrived, storage became an issue, and equipment was stored in office space and around workstations, which created a potential safety and fire hazard. In Summer 2010, an IP official was tasked with reviewing the amount of equipment being stored and determined that ISCD was "stockpiling" fire-retardant suits, uniforms, laptops, printers, and flashlights, as well as other items. The justification given to this official by ISCD was to have new inspectors equipped when hired. The IP official said that it would be impossible to recruit enough inspectors at one time to use all the equipment and supplies, and was concerned that the equipment might expire or become obsolete before ISCD could assign it.

In Spring 2011, ISCD began transferring unnecessary, excessive, or outdated equipment to other offices within NPPD or the Department. Approximately \$700,000 in equipment and uniforms was transferred in FY 2011 and FY 2012. However, ISCD did not receive any compensation for transferred items. Most transfers were informally initiated and confirmed through email messages to specify types and quantity of equipment needed. In some instances, the equipment was ordered, received, and transferred in its entirety. For example, one complete purchase request for hazardous material equipment ordered August 2, 2010, was transferred to FPS on May 2, 2011. The value of that order was \$165,072.25.

ISCD's Vehicle Leases Led to Possible Misuse and Wasted Funds

ISCD Chemical Security Inspectors use leased vehicles to conduct site visits, inspections, outreach, enforcement, and other compliance-related activities. Similar to the justification for equipment purchases, ISCD obtained leased vehicles through the General Services Administration in large numbers to ensure that inspectors would have a vehicle when hired.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In August 2009, however, concerns were raised within IP and NPPD about the number of vehicles leased by ISCD. ISCD received an email message from NPPD's Office of Budget stating,

You currently have 84 vehicles, and are requesting 70 additional vehicles in FY 2010 and 70 in FY 2011. While the additional 70 in FY 2010 makes sense compared to the number of inspectors requested in the budget, the additional 70 in FY 2011 does not, because you did not request additional staff for ISCD.

In 2010, IP again raised concerns when ISCD was planning to move its headquarters to a new location and requested a large number of vehicle parking spaces. In June 2010, the IP Assistant Secretary established a centralized fleet management task force within IP to ensure that specific usage controls and reporting requirements were being followed. Monitoring and oversight of ISCD's vehicles led to the prohibition of headquarters staff using vehicles for home-to-work purposes and eliminated the headquarters pool of vehicles.

In 2011, ISCD transferred 33 leased vehicles to U.S. Citizenship and Immigration Services, FPS, and another departmental office because ISCD no longer needed the vehicles. These were transfers of accountability without an exchange of funds. However, the lease cost to ISCD for the 33 vehicles was more than \$108,000 annually. As of October 2012, ISCD has 104 leased vehicles assigned to field personnel only. In July 2012, NPPD issued the Motor Vehicle Fleet Management Program directive and manual to all employees.

ISCD Initially Requested Open Secret Storage Space but Determined It Was Unnecessary

ISCD's initial headquarters location provided it with access to classified space. When ISCD relocated in 2010, it requested that similar access be built into new office space. In early 2012, however, ISCD determined that the office classification level exceeds work area requirements, limits its ability to interact with industry partners, and hinders coordination necessary to conduct compliance reviews.

ISCD officials said employees require regular access to classified information to fulfill its mission effectively. This includes access to various classified information and analysis, infrastructure tier and priority lists, and other classified products appropriate to IP's missions. As a result, ISCD requested that its space be open secret storage to house classified systems at the secret level as well as to house



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

a Sensitive Compartmented Information Facility.⁴⁰ DHS Management Directive 11046 defines open secret storage as a room or area constructed and operated for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers. The office was built in 2010 to ISCD requirements for approximately \$5.5 million. This included \$2.4 million in physical upgrades, \$1.2 million for additional guard service, and \$1.9 million for information technology costs associated with the build-out.

In early 2012, after occupying the new space for less than 2 years, ISCD officials determined that only one of three floors should remain classified space. Several ISCD employees said the space should not have been classified, as they never handle classified material. The estimated cost to declassify the open storage space is \$122,000, which includes removing and replacing desktops, performing data migration, reconfiguring telephones, and removing and relocating network equipment.

Recommendation

We recommend that the Assistant Secretary for Infrastructure Protection:

Recommendation #20:

Establish internal controls to ensure accountability for all ISCD appropriated funds and that sufficient justification exists for all procurements.

Management Comments and OIG Analysis

Management Comments to Recommendation #20: NPPD officials concurred with Recommendation 20. In its response, NPPD said that ISCD has established several internal controls and approval forms to ensure appropriate funding accountability. Within the Annual Operating Plan, ISCD has established metrics that allow for ISCD leadership to see quarterly updates on the division's progress towards meeting this accountability objective. As the owner of the Annual Operating Plan, the ISCD Program Management Office has developed formal objectives to help ensure the appropriated funds are accounted for and

⁴⁰ A Sensitive Compartmented Information Facility is an accredited area, room, group of rooms, buildings, or installation where Sensitive Compartmented Information may be stored, used, discussed, and/or processed. Sensitive Compartmented Information is classified information concerning or derived from intelligence sources, methods, or analytical processes.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

expended as necessary. ISCD works to ensure less than or equal to a 10 percent variance between appropriated funding and obligated funding within the current fiscal year. Working under 1 year funds, ISCD ensures procurements are executed as planned and within the funding limits. The procurement administrative lead timelines are also tracked, and ISCD works to achieve a 95 percent or higher completion rate of procurements within the Office of Procurement Operations procurement administrative lead timelines guidelines.

ISCD also recently implemented an Acquisition Justification Form to be used internally for funding requests for approval. The form includes requirement descriptions, funding amounts, and mitigation strategies in the event of disapproval. The form ensures execution alignment with the ISCD fiscal year spend plan in coordination with IP. The spend plan is a tracking means for the division as well as IP to properly fund each quarter based on requirement needs. Contractor performance and fund expenditure rates are closely monitored via cost and schedule reports, and periodic project and technical management reviews. In addition, billing submissions are scrutinized and planned performance objectives are compared with actual results.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 20, which is resolved and open. This recommendation will remain open pending our receipt of ISCD's procurement administrative lead timelines reporting and the Acquisition Justification Form.



Dysfunctional Culture Contributed to Perceptions of Retaliation and Suppression of Nonconforming Opinions Within ISCD

Although we were unable to substantiate any claims of retaliation or suppression of nonconforming opinions, the ISCD work environment and culture cultivates this perception. Constant turnover in leadership, reorganizations, and personality conflicts impair effective work relationships. In addition, the negative tone of the leaked internal ISCD memorandum decreased morale within the division.

Revolving Leadership Resulted in Constant Program Changes

Since 2006, ISCD has had eight directors, resulting in constant changes to CFATS Program processes, procedures, oversight, and implementation. Several ISCD staff said that it can potentially take more than 5 months to acclimate new leadership to ISCD and the CFATS Program. Both ISCD Director and Deputy Director positions, as well as branch chief and deputy branch chief positions, have been filled by acting personnel. Appendix G shows a 2009 memorandum to all IP employees, which illustrates the cascading effect that IP leadership vacancies has had on IP divisions such as ISCD. Multiple permanent branch chiefs were appointed to acting Director or Deputy Director positions, requiring some employees to perform both acting and permanent leadership position duties and responsibilities.

Several ISCD employees cite limited transparency and poor communication across the division, and limited communication within and between branches at headquarters. For example, there is little guidance on processes and procedures, primarily because acting managers do not want to make decisions. As a result of the multiple reorganizations and high attrition, several ISCD employees are not always certain of the supervisory reporting structure.

Some ISCD employees said reorganizations were often executed for nonprogrammatic reasons. Employees perceived cliques forming, which led to favoritism and placing people in positions without merit or qualification. ISCD employees said that the work culture within the division was frequently combative because there was confrontation among division leaders. As a result, employees frequently did not want to voice nonconforming opinions. In addition, employees complained of unprofessional senior staff behavior, such as use of profanity, inappropriate relationships, and violent outbursts. Many ISCD employees felt that there was little accountability in the division and that people who performed poorly were often rewarded with better positions, details, and educational opportunities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ISCD has placed lower-graded personnel into acting positions, which may require them to supervise higher-graded personnel. While we were unable to determine what restrictions may apply to this type of assignment, it is sound business practice that a supervisor's grade should be equal to or greater than that of subordinates. In addition, such situations have fostered resentment among employees.

After the memorandum release, some ISCD employees said that it was "a slap in the face" and they felt insulted, degraded, and betrayed by their portrayal in the memorandum. Many Chemical Security Inspectors said they were targeted by ISCD leadership and offended by how inspectors were portrayed as being unprofessional and unqualified. In addition, inspectors said their image had been tarnished within the chemical industry. ISCD staff asked to see the memorandum, but were denied. Since the memorandum was not distributed to all employees, knowledge of its content was limited to what they learned from news reports and subsequent congressional hearings. Many ISCD employees expressed frustration that news media and chemical industry representatives obtained copies but employees did not.

During our fieldwork, ISCD leadership proposed another realignment that would change position job series for some employees. Employees said this would require recompetition for their jobs, with the possibility that they might not qualify. Also, several ISCD management officials in acting positions said they would not apply for their positions when advertised as permanent, for either professional or personal reasons.

Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #21:

Advertise and select permanent ISCD leadership with demonstrated qualifications and skills at all levels, to include Division Director, Deputy Division Director, branch chiefs, deputy branch chiefs, and section chiefs.

Recommendation #22:

Develop and disseminate an ISCD organizational and reporting structure to all ISCD staff.



Management Comments and OIG Analysis

Management Response to Recommendation #21: NPPD officials concurred with Recommendation 21. In its response, NPPD said they agree that having a permanent, qualified ISCD leadership team is critical to the long-term success of the CFATS Program, and have been working towards that end over the past few months. ISCD has filled or is in the process of filling all ISCD leadership positions with permanent, qualified individuals.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 21, which is resolved and open. This recommendation will remain open pending our receipt of documentation that ISCD leadership positions are filled with permanent, qualified individuals.

Management Response to Recommendation #22: NPPD officials concurred with Recommendation 22. In its response, NPPD said the ISCD Director disseminated on January 14, 2013, an ISCD organizational chart to all ISCD staff that included the ISCD reporting structure.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 22, which is resolved and open. This recommendation will remain open pending dissemination of the ISCD organizational and reporting structure to all ISCD staff once leadership positions have been filled with permanent, qualified individuals.

NPPD Has a Process To Report Allegations, but DHS OIG Contact Information Is Outdated

In November 2011, NPPD's Under Secretary sent a memorandum to all employees explaining how they should report misconduct allegations. The memorandum was also a reminder that all NPPD employees have a responsibility to report misconduct allegations and described the types of allegations that employees must report to DHS OIG or OCS, as well as allegations that supervisors should handle. Contact information for reporting matters to OIG or OCS was included, and contained an email address for the DHS OIG Hotline.

However, DHS OIG no longer uses an email address to receive reports. Some ISCD employees said that they sent email messages to the hotline and did not receive a response. These employees assumed the hotline had received their allegations, but DHS OIG had no record of those complaints. We tested the email address and did not receive a reply confirming receipt or that the email address is no longer valid. Nor did we receive a response redirecting us to the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

DHS OIG website to report allegations. According to the DHS OIG website, reports can now be made by completing the OIG allegation form, calling a toll-free number, faxing, or mailing the allegation information as indicated.

Online: Allegation Form (Recommended)
Call: 1-800-323-8603 toll free
Fax: 202-254-4297
U.S. Mail: DHS Office of Inspector General
Attention: Office of Investigations Hotline
245 Murray Drive SW
Building 410/Mail Stop 2600
Washington, DC 20528

Despite receiving guidance on how to report misconduct allegations to OIG or OCS, many ISCD employees said they did not know how to report a complaint.

To address issues with reporting misconduct allegations, DHS OIG will disseminate to all DHS employees current procedures for reporting misconduct allegations to the DHS OIG within 30 days of the issuance of this report.

Recommendation

We recommend that NPPD's Under Secretary:

Recommendation #23:

Reiterate to all NPPD employees the process for reporting misconduct allegations.

Management Comments and OIG Analysis

Management Response to Recommendation #23: NPPD officials concurred with Recommendation 23. In its response, NPPD said the Under Secretary disseminated on January 16, 2013, a message to all NPPD employees announcing the implementation of the Principles of Integrity and Professional Responsibility Management Directive. Included in that message were the reporting procedures for employees to submit allegations of misconduct. Additionally, the NPPD OCS has updated its website to include the proper procedures and contact information for reporting allegations of misconduct. NPPD intends to continue to reiterate regularly the reporting procedures to its employees and NPPD OCS is working with the Public Affairs Office to draft an updated memorandum or message to all employees.



OIG Analysis: We consider NPPD's actions responsive to Recommendation #23, which is resolved and open. This recommendation will remain open pending our receipt of the January 16, 2013, message disseminated to all NPPD employees and updated memorandum or message drafted by the Public Affairs Office.

Industry Supports the CFATS Program, but Challenges Remain and Corrective Action Is Necessary

The regulated chemical industry has embraced the RBPS approach and the flexibility it allows; however, constant ISCD leadership changes have strained its relationship with the regulated community. In addition, challenges remain with CSAT tools and limited feedback is provided to facilities following submissions of SVAs and SSPs. While the industry has applauded ISCD leadership for identifying programmatic issues, additional efforts are necessary. Industry officials support the CFATS Program but are concerned about industry resources and funds spent to meet program requirements without a clear path forward.

Excessive Leadership Changes Have Strained ISCD's Relationship With the Regulated Community and Impede CFATS Program Progress

Industry officials said when ISCD and IP established the CFATS Program, it was overly dependent on a small group of IP officials, detailees, and contractors. In addition, continuous turnover throughout ISCD requires industry officials to repeatedly engage new leadership and program staff to convey industry needs, concerns, and expectations. Because of extensive turnover, industry officials said CFATS is no closer to implementation, and most of the ISCD senior officials with whom industry worked during CFATS Program development are no longer with the program, making it difficult to build relationships and impedes program progress. Industry officials also expressed concern over the small number ISCD employees possessing chemical industry knowledge.

Industry officials are encouraged, however, to have a permanent ISCD director as of July 2011, and said current leadership appears capable and willing to work with the industry, though this varies at the ISCD staff level.

Industry Is Concerned by Limited Transparency and Slow Implementation of the CFATS Program

There has been limited communication from ISCD to industry regarding how facilities are tier assigned, and comments from ISCD on submitted materials has not been timely. Most industry officials we spoke with are confused by how



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ISCD assigns risk-based tiers to their facilities, as some are higher and others lower than expected. ISCD does not share the calculations used for facility tiering with industry officials. This is contrary to many security vulnerability assessment practices, where this information is transparent and used to inform decision makers of the best steps to take to manage risk. Additionally, industry decision makers often require a risk analysis to justify budget requests for those risk-reduction measures. In the CFATS process, the facility is not aware of how:

- Information submitted to DHS relates to actual security posture or potential gaps in security at the facility level;
- DHS is analyzing the information provided by facilities;
- Tiering decisions are made; and
- Any changes that might be made to the facility would affect tier level.

Unlike many industry vulnerability assessment methods, the CFATS model is mostly a data collection step for DHS' use and does not directly provide useful information to the facility on threats, vulnerabilities, consequences, or assist in identifying additional security needs. As a result, the SVA does not provide chemical facilities meaningful information for planning and executing an overall site security plan with a coherent resource estimate. Industry does not understand the secrecy behind the CFATS model or its CSAT tools.

Industry officials said it seemed that people developing the CFATS Program thought chemical facilities were simple; as though each facility had one plant and required one fence. In reality, there are sites that encompass 10,000 acres, with multiple plants making a variety of products with multiple chemicals. Industry representatives were concerned whether CFATS has enough qualified personnel to review SSPs.

While industry representatives generally support the CFATS Program, its slow implementation has caused additional concern. Industry views the CFATS Program as excessive paperwork and resource intensive. SSPs can range from 300 to more than 1,000 pages and take a facility days to weeks to complete, even with multiple staff involved. There are deadlines for industry; however, DHS has not met its deadlines as stated in the CFATS regulation. For example, an industry official said a facility has removed its COI and requested redetermination from the Department 2 years ago, but has not received a decision, even though a decision should be provided within 45 days.

Some industry security representatives thought that the CFATS Program would be implemented on an aggressive timeline and obtained corporate support to invest in facility upgrades. Security officials have lost momentum in securing



corporate funds for facility upgrades because of the slow implementation of the CFATS Program.

After the internal ISCD memorandum was leaked to news media in December 2011, Congress provided some industry members with copies. Overall, industry representatives were not surprised by the results, nor did their perspective of the program change. Industry representatives have testified before Congress that the reported issues in the leaked internal memorandum are not insurmountable.

Recommendation

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #24:

Improve the clarity of guidance provided to the CFATS-regulated industry so that it can benefit from regular and timely comments on facility submissions.

Management Comments and OIG Analysis

Management Response to Recommendation #24: NPPD officials concurred with Recommendation 24. In its response, NPPD said that as part of its efforts to improve the CSAT, ISCD intends to update its guidance materials for the Top-Screen, SVA, and SSP. ISCD is also in the process of developing updated guidance related to its Chemical-terrorism Vulnerability Information Program, and intends to release guidance specific to the CFATS Personnel Surety Program when the CFATS Personnel Surety Program is launched. Finally, ISCD intends to routinely update its website and Frequently Asked Questions page based on user feedback to provide clear guidance and assistance to the regulated community.

OIG Analysis: We consider NPPD's actions responsive to Recommendation 24, which is resolved and open. This recommendation will remain open pending our receipt of its guidance materials for the Top-Screen, SVA, SSP, Chemical-terrorism Vulnerability Information Program, and the CFATS Personnel Surety Program.



Conclusion

DHS established the CFATS Program as required by the *Department of Homeland Security Appropriations Act of 2007*, to regulate chemical facilities that may present a high-level security risk. NPPD's ISCD is responsible for implementing the CFATS Program. ISCD's action plan addressed some issues contained in the December 2011 leaked internal memorandum; however, challenges remain. For example, ISCD needs to improve program-related tools and processes, reduce reliance on contractors, eliminate program waste and duplication, follow proper hiring practices, and provide sufficient training to personnel at all CFATS Program levels. ISCD can enhance program efficiency and effectiveness by addressing these challenges.



Appendix A

Objectives, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

DHS regulates chemical facilities that may present a high-level security risk through the CFATS Program. ISCD, within NPPD, is responsible for CFATS implementation. In December 2011, an ISCD limited distribution memorandum was leaked to news media. This memorandum disclosed allegations of employee misconduct and inadequate performance, as well as misuse of funds and ineffective hiring within the CFATS Program. In February 2012, former Chairman Lungren, of the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, requested that we review these issues. In April 2012, Ranking Member Waxman, of the House Committee on Energy and Commerce, also requested that we review the challenges facing the CFATS Program. We consolidated both requests into one review.

Our objectives were to determine whether: (1) management controls are in place and operational to ensure that the CFATS Program is not mismanaged; (2) NPPD and ISCD leadership misrepresented CFATS Program progress; and (3) nonconforming opinions of CFATS Program personnel have been suppressed or met with retaliation.

We reviewed relevant legislation, regulations, directives, policies, strategic plans, annual reports, and congressional testimony, and collected program documents, including budgets, official guidance and emails, training materials, performance metrics, guidelines, operating procedures, and human resources documents. We also studied work previously performed by our office and the Government Accountability Office (GAO).

We interviewed NPPD, IP, and ISCD personnel responsible for CFATS Program implementation and oversight. We also interviewed union and industry officials to gain their perspectives on the CFATS Program. To develop an understanding of similar programs, we interviewed USCG officials to discuss challenges and best practices they experienced in implementing the *Maritime Transportation Security Act of 2002*.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Our fieldwork began in May 2012 and concluded in October 2012. We conducted this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.



Appendix B

Recommendations

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #1:

Modify Chemical Security Assessment Tools to capture facility data efficiently and ensure that the tools provide meaningful end products for industry users and ISCD.

Recommendation #2:

Document engagement with Office of Infrastructure Protection and DHS regulatory and voluntary programs to identify and implement existing tools and processes that can be leveraged to make Top Screen, Security Vulnerability Assessments, and the Site Security Plan tools more efficient, effective, and easier to use for the CFATS Program.

Recommendation #3:

Provide evidence of how the revised long-term Site Security Plan review process has reduced the Site Security Plan backlog for all tiers.

Recommendation #4:

Define, develop, and implement processes and procedures for Compliance Inspections, and train CFATS personnel to conduct Compliance Inspections.

Recommendation #5:

Identify and implement a process to improve the timeliness of ISCD determinations for all facility submissions.

Recommendation #6:

Develop a strategy and implement a plan to address facility resubmissions and requests for redetermination as prescribed in the CFATS regulation.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation #7:

Limit funding for Personnel Surety Program vetting until the Office of Management and Budget has approved the program's Information Collection Request.

Recommendation #8:

Develop an action plan and guidance for implementing the Ammonium Nitrate Program, which incorporates lessons learned from CFATS Program challenges.

Recommendation #9:

Develop and implement a curriculum and timeline for training inspectors to perform both Ammonium Nitrate and CFATS Program duties and responsibilities.

Recommendation #10:

Develop and implement program metrics that measure CFATS Program value accurately and demonstrate the extent to which risk has been reduced at regulated facilities.

Recommendation #11:

Develop a strategy and implement a plan to work with Congress and private industry to ensure long-term authorization for the CFATS Program.

Recommendation #12:

Develop a methodology and reporting process to identify and address errors and anomalies that arise in the CFATS tiering methodology and risk engine.

Recommendation #13:

Provide the external peer review results, including comments on the V Factor, and ISCD's action plan to implement external peer review recommendations.

Recommendation #14:

Reduce overall ISCD reliance on contract personnel to avoid the appearance that contractors may be performing inherently governmental functions and closely associated governmental functions.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation #15:

Develop and implement a learning curriculum that (1) describes position roles and responsibilities clearly; (2) provides comprehensive training plans to prepare employees to perform assigned duties; and (3) communicates measures to assess performance.

We recommend that the Director of NPPD's Office of Human Capital:

Recommendation #16:

Develop NPPD-wide policy regarding appointment of acting management in accordance with Office of Personnel Management guidelines.

Recommendation #17:

Ensure that all employees serving in an acting supervisory capacity have a supervisory position description in accordance with Office of Personnel Management requirements.

Recommendation #18:

Ensure that all employees receive performance reviews according to NPPD's General Instruction Guide on performance management.

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #19:

Eliminate the authorization and payment of Administratively Uncontrollable Overtime for all ISCD personnel.

We recommend that the Assistant Secretary for Infrastructure Protection:

Recommendation #20:

Establish internal controls to ensure accountability for all ISCD appropriated funds and that sufficient justification exists for all procurements.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #21:

Advertise and select permanent ISCD leadership with demonstrated qualifications and skills at all levels, to include Division Director, Deputy Division Director, branch chiefs, deputy branch chiefs, and section chiefs.

Recommendation #22:

Develop and disseminate an ISCD organizational and reporting structure to all ISCD staff.

We recommend that NPPD's Under Secretary:

Recommendation #23:

Reiterate to all NPPD employees the process for reporting misconduct allegations.

We recommend that the Director of the Infrastructure Security Compliance Division:

Recommendation #24:

Improve the clarity of guidance provided to the CFATS-regulated industry so that it can benefit from regular and timely comments on facility submissions.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C Management Comments to the Draft Report

Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528



Homeland
Security

MAR 14 2013

Mr. Charles K. Edwards
Deputy Inspector General
Office of Inspector General
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Edwards:

Re: Office of Inspector General Report, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (OIG Project No. 12-139-ISP-NPPD)

Thank you for the opportunity to review and comment on the draft Office of Inspector General Report, *Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program* (OIG Project No. 12-139-ISP-NPPD) (hereafter referred to as the "OIG Report" or the "Report"). The U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP), and Infrastructure Security Compliance Division (ISCD) [hereinafter collectively referred to as NPPD] acknowledge the significant effort undertaken by the Office of Inspector General (OIG) in planning and conducting its review and issuing this report. The success of the Chemical Facility Anti-Terrorism Standards (CFATS) Program is a top priority for NPPD, and we welcome external perspectives on how to improve this important homeland security program.

We understand that an already difficult task of reviewing a complex program was made more challenging by the effort of the OIG to de-conflict its assessment with two reviews of the same program that Congress had asked the Government Accounting Office (GAO) to undertake. As a result of this potential conflict, the OIG Report states that the scope of their review was to the end of fiscal year 2012 only. In addition, the OIG explained that they did not attempt to include progress made on the Action Plan that ISCD leadership had developed in late 2011 and has nearly completed. Unfortunately, the decision to undertake what is now an historical review, along with the admitted lack of balance, necessarily diminishes the value and relevance of many of the issues and findings discussed in the Report.

NPPD has already taken many steps to address the issues and concerns raised in the Report, nearly all of which were first raised in an internal memorandum prepared in 2011 by ISCD leadership. Indeed, as part of the 2011 memorandum, ISCD leadership developed a comprehensive Action Plan that addressed the issues they had identified. Of the 95 items in the ISCD Action Plan designed to address these issues, 88 have already been implemented, leading



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

to significant improvements in the management of CFATS. This important progress is not acknowledged in the Report.

For example, the Report does not mention that the program has implemented a revised Site Security Plan (SSP) review process that has significantly increased the pace of SSP reviews, and re-trained inspectors on updated inspection protocols, which has led to a dramatic increase in the Authorization Inspection pace. In addition, ISCD has documented many critical processes through Standard Operating Procedures (SOPs). As described in greater detail below, as of March 8, 2013, these efforts have enabled ISCD to authorize 263 SSPs, conduct 131 Authorization Inspections, and approve 47 SSPs, including Alternative Security Programs (ASP). ISCD is now 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 we move into Tier 3 and Tier 4 SSP reviews.

Given the alignment of many of the issues discussed in the OIG Report and the 2011 Action Plan, NPPD agrees with a majority of the OIG recommendations and, in fact, has already taken action to close six recommendations. NPPD does not concur with four of the recommendations and will address them below. Moreover, NPPD has significant concerns with the accuracy of several of the OIG findings, the unsubstantiated nature of many of the allegations contained within, and the OIG's failure to interview key personnel on issues within their portfolios during the period under review. Each of these concerns will be discussed in greater detail.

OIG Recommendations Already Addressed in the ISCD Action Plan

Many of the OIG concerns and recommendations are addressed, in whole or in part, by items in the 2011 ISCD Action Plan. Below is a list of Action Plan tasks that have been completed, with the relevant OIG recommendation included in a parenthetical after each action item.

- Initiate the hiring process to fill gaps in required skill sets and experience (*OIG Recommendation 21*)
- Engage the IP Director of Management's Office and NPPD Office of Human Capital to expedite the vacancy announcements for Branch Chief positions (*OIG Recommendation 21*)
- Implement a series of all-hands meetings within ISCD to provide the team with clarity concerning priorities, to lay the groundwork for a change in culture, and to involve the team in solving challenges facing the Division (*Addresses concerns regarding effectiveness of internal communications and Division culture*)
- Collect surveys from attendees at all-hands meetings identifying perceptions of our greatest strengths, our greatest challenges, and recommendations for the way forward; analyze the results of the employee surveys to identify the major themes; and develop a plan to address them (*Addresses concerns regarding effectiveness of internal communications and Division culture*)
- Establish transparent and effective communication with the workforce on important issues such as program changes, promotions, projects, and similar items (*OIG Recommendation 22*)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Communicate DHS policy with regard to performance management to all employees and appropriately address any reports of poor performance (*OIG Recommendation 18*)
- Improve messaging about the current status of the program, using consistent terminology to avoid confusion (*Addresses concern about use of confusing terminology leading to misunderstandings*)
- Codify the inspection methodology and associated procedures, appropriate forms and reporting methods, associated IT tools, equipment, guidance materials, and functional inspector training (*OIG Recommendations 1, 4, 9, 15*)
- Develop and implement an effective basic inspector training course; ensure all inspectors, current and new hires, attend the course; and ensure all inspectors receive updated training for inspections and an inspector training program is developed for new hires (*OIG Recommendations 4, 9, 15*)
- Develop and implement a plan to improve the Site Security Plan (SSP) review process (*OIG Recommendation 3*)
- Revise criteria for the scheduling of compliance inspections (*OIG Recommendation 4*)
- Revise the Chemical Security Assessment Tool (CSAT) to create a more efficient and effective tool for both industry and ISCD based on industry engagement (*OIG Recommendation 1*)
- Evaluate all current and planned contracts using the DHS Balanced Workforce Strategy and develop a plan to transition to Federal employees as appropriate (*OIG Recommendation 14*)
- Establish and implement a process for assessing Contracting Officer's Representative performance of contract administration responsibilities to ensure that contracts will continue to be developed, implemented, and overseen in a manner consistent with policy and law (*OIG Recommendation 14*)
- Engage NPPD and IP Offices of Human Capital concerning responsiveness to human capital issues and propose a bi-weekly meeting among ISCD and NPPD and IP Offices of Human Capital to ensure effective communications and visibility on issues (*OIG Recommendations 17, 18*)
- Effectively communicate to supervisors and managers the importance of compliance with the NPPD Performance Management Program; establish a tracking mechanism to ensure compliance, and hold supervisors and managers accountable for non-compliance with established standards for performance management (*OIG Recommendation 18*)
- Establish a process to evaluate any new requirements (*OIG Recommendation 20*)
- Review whether and to what extent the use of Administratively Uncontrollable Overtime (AUO) is appropriate within ISCD (*OIG Recommendation 19*)

Specific Areas of Greatest Concern with the OIG Report

The following are three areas contained in the OIG Report which NPPD believes are not supported by evidence and with which we strongly disagree.



Unsubstantiated Allegations of Suppression and Retaliation

The OIG Report acknowledges that it was unable to substantiate any claims of retaliation and suppression of nonconforming opinions. Despite this, the Report alleges, without supporting evidence, that the ISCD “work environment and culture cultivates this perception.” Given the unsubstantiated nature of this conclusion, it is difficult to assess. After identifying this as a potential issue in the 2011 internal memorandum, ISCD leadership has undertaken concerted efforts to provide an environment of openness and transparency, where individuals at all levels within the Division are encouraged to provide their opinions to ISCD leadership. In addition, NPPD has consistently worked to communicate to employees that leadership welcomes all view points and affirmatively encourages reporting of bad news to ensure that problems can be addressed in an appropriate and timely manner. The ISCD Director has taken steps to ensure that employee views and opinions are solicited and heard, including instituting an “open door” policy, conducting frequent all-hands meetings, and establishing a Director’s Advisory Working Group composed of staff-level employees from throughout the Division. Further, NPPD has established a “Suggestions” email inbox and periodically reminds employees of the avenues available to them to report allegations of misconduct and potential cases of fraud, waste and abuse, including the issuance of a Principles of Integrity and Professional Responsibility Management Directive in January 2013. NPPD will continue to work on this with the aim of assuring each and every employee that nonconforming opinions will not face suppression or retaliation.

Personnel Surety Program

In its review of the CFATS Personnel Surety Program, the OIG did not interview either the CFATS Personnel Surety Program Manager or representatives of the Department’s Screening Coordination Office (SCO) responsible for coordinating with ISCD on the development of the CFATS Personnel Surety Program. NPPD has offered to make the CFATS Personnel Surety Program manager available for interview to discuss the issues raised in the Report. The OIG elected not to do so.

The OIG Report suggests that the Terrorist Screening Center (TSC) can provide the same services as TSA and CBP through a no-cost detailee. In actuality, the services being procured by NPPD from TSA are much broader than basic TSDB vetting. For instance, TSA supports recurrent vetting, which is a DHS best practice, because it has substantially more security value than point-in-time vetting. TSC does not support recurrent vetting. TSA also can verify an individual’s enrollment in the Transportation Worker Identification Credential (TWIC) program or the Hazardous Materials Endorsement (HME) program, whereas TSC cannot. Similarly, only CBP can verify an individual’s enrollment in the Trusted Traveler Programs. Accordingly, NPPD has established an agreement with CBP to provide that service.

The OIG Report also states “Some ISCD staff said they wanted to identify alternate ways to conduct TSDB searches, but were prohibited from doing so.” In fact, as acknowledged in the Report, ISCD, IP, and NPPD have repeatedly explored alternatives to using TSA for TSDB vetting. On several occasions over the past three years, the CFATS Personnel Surety Program Manager was tasked by Division leadership with reviewing available alternatives and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

encouraged to seek other options. In doing so, the CFATS Personnel Surety Program Manager met with the TSC, Federal Protective Service, US-VISIT, and the Nuclear Regulatory Commission, among others. Each time the analysis supported the selection of TSA as the best vetting solution for NPPD.

Finally, the OIG Report does not acknowledge the DHS-wide effort, with which NPPD has aligned, to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities related to screening activities involving the TSDB. In particular, the OIG Report omits that DHS and TSC have established a process for transmitting TSDB data from TSC to DHS through a service called the “DHS Watchlist Service” (WLS). Under the WLS, TSC, who remains the authoritative source of watchlist data, provides DHS with near real-time synchronization of the TSDB. DHS then uses the data in the WLS to support DHS TSDB screening activities. As a result, the statement that ISCD “cannot identify individuals with terrorist ties without TSC information” is somewhat misleading. Rather, the Department has made substantial investments to make available a copy of the TSDB for use by DHS components, and thus those components do not need to go directly to TSC for that information.

Overall, the Personnel Surety Program discussion in the OIG Report has a number of inaccuracies and fails to discuss various considerations, factors, and constraints that influence how, when, and to whom funding for the CFATS Personnel Surety Program historically has been allocated and will be allocated in the future. Consequently, NPPD cannot support the recommendation related to the CFATS Personnel Surety Program.

Inherently Governmental Functions

The OIG Report states that IG was “unable to substantiate whether contractors were performing inherently governmental functions.” The Report enumerates a number of categories of activities that generically meet the definition of inherently governmental functions and closely associated governmental functions, but the IG did not find any activities that were actually performed by ISCD contractors that would meet the definition of an inherently governmental function. The Report notes that contractors developed training material, which is not an inherently governmental function.

The OIG Report similarly fails to provide any specific examples of closely associated governmental functions performed by ISCD contractors. The OIG does assert that ISCD does not always have the minimum percentage of Federal employees needed to perform or oversee these functions, although it does not provide any examples. Rather, the OIG cites the perception of insufficient Federal supervision on a single, anonymous employee.

The OIG Report also fails to acknowledge the mechanisms that NPPD has in place to ensure that its contractors do not perform inherently governmental functions and, thereby, to ensure compliance with applicable laws and regulations. For example, all NPPD contracts are vetted under the Department’s Balanced Workforce Strategy. This process includes a review of all Statements of Work (SOW) to ensure that no work contained in the SOW is inherently governmental.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response to Recommendations

NPPD previously provided technical comments and corrections of factual errors to OIG under separate cover. With regard to recommendations, we agree in whole or in part with all but four of the 24 recommendations. Notably, ISCD identified similar action items nearly 18 months ago and included them in the Action Plan. NPPD has already taken actions that complete six of the recommendations, and has made significant progress towards completion of a number of other recommendations as well. Below are NPPD's detailed responses to the 24 recommendations contained in the OIG Report.

Recommendation 1: Modify Chemical Security Assessment Tools to capture facility data efficiently and ensure that the tools provide meaningful end products for industry users and ISCD.

Response: Concur. Improving the Chemical Security Assessment Tool (CSAT) is one of ISCD's top priorities for fiscal years (FY) 2013 and 2014. Based on input received to date from both the regulated community as well as internal ISCD users of the outputs of the CSAT applications, ISCD has identified a number of potential improvements that should help make all three of the primary CSAT applications—the Top-Screen, the Security Vulnerability Assessment (SVA), and the SSP—more user-friendly, more efficient, and more effective. Some of the currently envisioned changes to the CSAT tool include improved question quality and question flow; pre-population of data within the tool to reduce the burden on industry users and minimize the likelihood of data entry errors; dynamic lists of options and forced selections to expand pre-defined responses to questions to reduce the collection of unstructured text in “other” fields; and preparation of a CSAT tool lexicon and on-screen (i.e., contextual) help to better lead and instruct CSAT users.

In order to revalidate and formalize those suggestions for improving CSAT as well as identify any additional potential improvements, ISCD launched a “CSAT re-engineering and optimization” effort in 2012. This effort was broken into four tasks: formally engage the regulated community to solicit industry feedback and increase stakeholder involvement and buy-in; refine and document the process model for the lifecycle of a facility submission; document functional requirements to address industry concerns and information technology (IT) architecture inefficiencies; and revise and implement the modified IT system.

ISCD has already initiated discussions regarding this effort and is soliciting input from members of the regulated community with which ISCD interacts on a regular basis. In order to expand the pool of entities providing feedback to better ensure all elements of the regulated community have a chance to contribute, the Department has scheduled three roundtables with members of the regulated community in various locations around the United States.

Recommendation 2: Document engagement with Office of Infrastructure Protection and DHS regulatory and voluntary programs to identify and implement existing tools and processes that can be leveraged to make Top Screen, Security Vulnerability Assessments, and the Site Security Plan tools more efficient, effective, and easier to use for the CFATS Program.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. NPPD agrees that documenting engagement between DHS regulatory and voluntary programs to identify and, where appropriate, implement existing tools and processes that can be leveraged to make the CFATS program more efficient and effective is a worthwhile goal and we are committed to doing so. We do, however, strongly disagree with the OIG implication that the voluntary and regulatory programs have not previously collaborated and the OIG claim that ISCD management has separated the IP voluntary and regulatory programs in a manner that impedes ISCD's ability to identify and apply best practices for its program.

While it is correct that ISCD leadership has strived to ensure that there is a bright line demarcating the regulatory and voluntary efforts, as is appropriate, ISCD leadership has also worked diligently through the years to ensure cross-Divisional awareness of efforts, collaboration across the voluntary and regulatory programs, and leveraging of tools and best practices where appropriate. This collaboration has occurred in a number of ways since the inception of ISCD.

For example, the information technology system used by ISCD to support the assessment of CFATS Site Security Plans is based on the system previously developed and still used by the Protective Security Advisors (PSAs) within IP's Protective Security Coordination Division (PSCD) to conduct vulnerability assessments. In fact, to best leverage the previous experiences gained in developing the tool used by the PSAs, ISCD hired primarily the same staff at Argonne National Laboratory to develop the CFATS SSP scoring tool. Similarly, when developing its cyber security standards in support of Risk-Based Performance Standard 8, ISCD established a team of cyber security experts led by representatives from the National Cyber Security Division (a predecessor to the Office of Cybersecurity and Communications). Third, when ISCD was determining how to incorporate threat into the CFATS risk methodology, ISCD consulted with the risk experts located in IP's HITRAC.

Throughout its history, ISCD also has worked routinely with IP's Sector Outreach and Programs Division (SOPD), in particular their Chemical Sector Specific Agency (SSA) and Oil & Natural Gas SSA. For instance, on numerous occasions throughout its history, various members of ISCD's leadership team have received briefings on the Chemical SSA's Voluntary Chemical Assessment Tool with an eye towards how it might be utilized to improve the CFATS assessment processes. Similarly, ISCD and PSCD leadership have met on a number of occasions to discuss how ISCD Chemical Security Inspectors and PSCD PSAs could collaborate better and how activities performed by each could be used to support efforts by the other's Division. For example, in April 2012, ISCD and PSCD leadership jointly met with a group of ISCD Field Commanders and PSCD Supervisory PSAs to discuss continued interaction between the two Divisions' field cadres and to identify opportunities for leveraging each cadre's activities throughout IP.

ISCD leadership and staff also participate in various recurring meetings with representatives from other IP divisions to, among other things, exchange ideas and best practices, discuss joint activities and programs, and provide status updates on Divisional activities. This includes a weekly IP leadership meeting involving the Assistant Secretary for Infrastructure Protection and Directors and/or Deputy Directors from all IP Divisions, and bi-weekly SOPD-led calls that focus on activities underway in the various critical infrastructure sectors.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation 3: Provide evidence of how the revised long-term Site Security Plan review process has reduced the Site Security Plan backlog for all tiers.

Response: Concur/Completed. The updated SSP authorization, inspection, and approval rates currently occurring, which are described below, demonstrate that the current updated SSP review process is reducing the SSP backlog for all tiers, beginning with Tiers 1 and 2.

During the first half of 2012, ISCD performed a number of activities that have significantly improved the pace of SSP reviews and inspections and reduced the SSP backlog. These activities include clarifying some of the policies regarding SSP reviews, finalizing the development of a new SSP review process, training SSP reviewers on the new process, developing a CFATS Inspections Standard Operating Procedure (SOP), and training the entire CFATS Chemical Security Inspector Cadre on the new inspections SOP. As a result of these and other complementary activities, the rate of SSP reviews, authorizations, and approvals, as well as the rate of conduct of Authorization Inspections, has significantly increased.

Specifically, as of September 1, 2012, ISCD had only authorized 60 SSPs, conducted 19 Authorization Inspections, and had not approved any SSPs. From October 2012 through January 2013, however, ISCD completed its review of all Tier 1 facility SSPs and authorized an average of 36 SSPs per month, with a high total of 47 authorizations in January 2013. ISCD is projecting authorizations to hold steady at this pace, with between 40 and 50 authorizations expected each month for the remainder of the fiscal year. With the number of authorized SSPs increasing, the number of Authorization Inspections being conducted is steadily increasing as well. ISCD completed 26 Authorization Inspections in January 2013 and 48 Authorization Inspections in February 2013. ISCD is projecting that 40 or more Authorization Inspections will be conducted each month for the remainder of FY 2013. SSP Approvals have also increased, and as of March 5, 2013, ISCD has approved SSPs (or ASPs submitted in lieu of SSPs) for 40 facilities. ISCD is projecting a steady increase in the number of approvals going forward as well, with between 30 and 50 per month expected to become the norm starting in March 2013.

ISCD intends to continue to track and report on these statistics, and believes they clearly demonstrate the revised SSP process and other improvements have dramatically increased SSP throughput and are reducing the SSP backlog.

Recommendation 4: Define, develop, and implement processes and procedures for Compliance Inspections, and train CFATS personnel to conduct Compliance Inspections.

Response: Concur. NPPD agrees that it is imperative to ensure that processes and procedures for scheduling and performing all CFATS inspections, including Compliance Inspections, are well documented and that CFATS personnel who conduct inspections are trained on how to properly conduct them. To that end, ISCD has developed a Standard Operating Procedure for Inspections of CFATS Covered Facilities, which defines the different types of inspections conducted by ISCD, enumerates roles and responsibilities related to inspections, and details processes and standard operating procedures for pre-inspection, inspection, and post-inspection activities.

During the summer of 2012, all of ISCD's CFATS Inspectors participated in one of five two-week training sessions on the new, documented ISCD Inspection protocols. These training



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

sessions enabled ISCD to resume Authorization Inspections in July 2012. Many of the lessons taught during these two-week sessions are equally applicable to Compliance Inspections. Nevertheless, it is ISCD's intention to provide additional training more specific to Compliance Inspections to all of its Chemical Security Inspectors prior to their beginning to conduct those inspections in September 2013.

Recommendation 5: Identify and implement a process to improve the timeliness of ISCD determinations for all facility submissions.

Response: Concur. NPPD recognizes that responding to facility submissions in a timely fashion is important for the credibility of the program and continues work to reduce response times. It is worth noting, however, that the OIG Report overstates the current average time frame it is taking ISCD to issue determinations based on Top-Screen and SVA submissions. Over the last three-month period measured, the average time from the facility's submission of an initial Top-Screen to ISCD's notification of a preliminary tier or non-regulated status is 64 days (not 4.8 months), the average time from the submission of an updated Top-Screen to notification of a revised tier or non-regulated status is 60 days (not 6.9 months), and the average time from the submission of an SVA to notification of a final tier or non-regulated status is 101 days (not 7.5 months).

Recommendation 6: Develop a strategy and implement a plan to address facility resubmissions and requests for redetermination as prescribed in the CFATS regulation.

Response: Concur. ISCD has established draft procedures and policies for receiving, reviewing, and responding to facility resubmissions and requests for redetermination. ISCD also has provided guidance to facilities on how to properly request a redetermination and file a resubmission, established criteria for how to effectively process the requests, and determined appropriate review and analysis channels. Each request is reviewed to determine if the resubmission significantly affects the facility's processes and chemicals or only has minor impacts. This determination allows ISCD to identify the appropriate next steps involving the facility, which may include a Compliance Assistance Visit, new tiering determination, updated SVA, updated SSP, and/or other action.

Recommendation 7: Limit funding for Personnel Surety Program vetting until the Office of Management and Budget has approved the program's Information Collection Request.

Response: Non-Concur. As noted earlier, the Personnel Surety Program discussion in the OIG Report contains a number of inaccuracies and fails to discuss many of the various considerations, factors, and constraints that influence how, when, and to whom funding for the CFATS Personnel Surety Program historically has been allocated and will be allocated in the future. As NPPD has done in the past, we will continue to perform careful and deliberate analysis prior to the expenditure of any funds related to the CFATS Personnel Surety Program and will only allocate funding when deemed appropriate given all relevant factors. The status of the Information Collection Request is simply one of those factors, albeit an important one. Consequently, the Department cannot concur with limiting funding to the Personnel Surety Program based solely on the status of the Information Collection Request without considering all of the other factors that go into the determination of how and when to fund the CFATS Personnel Surety Program.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation 8: Develop an action plan and guidance for implementing the Ammonium Nitrate Program, which incorporates lessons learned from CFATS Program challenges.

Response: Concur. As the Ammonium Nitrate (AN) Security Program is a proposed regulatory program, its development is guided in large part by the regulations and procedures set forth in the Administrative Procedure Act, the authorizing statute, and Office of Management and Budget (OMB) guidance with respect to rulemaking activities. NPPD has been working within the parameters established by those items to develop a final rule and an action plan and guidance for implementation of the final rule. NPPD/IP has recently assigned a member of the Senior Executive Service (SES) to oversee the development and implementation of the proposed Ammonium Nitrate Security Program.

Throughout the rulemaking and planning process, ISCD has been evaluating lessons learned from the CFATS Program and incorporating them into the development of the Ammonium Nitrate Security Program rulemaking activities and implementation planning. In particular, ISCD believes there are a number of programmatic similarities between the proposed Ammonium Nitrate Security Program and the proposed CFATS Personnel Surety Program. NPPD intends not only to apply lessons learned from CFATS Personnel Surety efforts to the Ammonium Nitrate Security Program, but also to take advantage of relationships, processes, information technology, and other aspects of the CFATS Personnel Surety Program to the maximum extent possible.

Recommendation 9: Develop and implement a curriculum and timeline for training inspectors to perform both Ammonium Nitrate and CFATS Program duties and responsibilities.

Response: Concur. ISCD is committed to ensuring that all personnel receive and maintain the appropriate level and scope of mission-specific training in support of CFATS and AN implementation. This includes training not only for inspectors, but also for those individuals performing compliance, policy and other activities in support of CFATS. Training for these personnel will be developed and executed over the next two years in a prioritized manner that best ensures our ability to complete our mission. In order to achieve this, among other things, ISCD intends to (a) analyze employee training needs and review, analyze, and update existing curriculum to improve learning content and outcomes; (b) assess and implement, as appropriate, blended learning technologies and curricula to include both Web-based / Distance Learning/ eClassroom solutions and traditional classrooms utilizing a variety of multi-media tools, including, but not limited to, webinars, training videos, and SharePoint collaboration tools; (c) design, develop, and deliver instructional content for all ISCD personnel based on roles, competencies, and learning objectives; and (d) evaluate training courses, curriculum and learning outcomes to ensure alignment with organizational priorities and enhance future training offered to ISCD employees.

In support of this effort, ISCD will develop, implement, update, and maintain training programs as required, using the Analysis, Design, Development, Implementation, and Evaluation (ADDIE) model of Instructional System Design (ISD) as the baseline framework. This framework will ensure that any training content is instructionally sound and adheres to DHS and federally approved technology standards and regulations (e.g., Sharable Content Object Reference Model



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

(SCORM), Section 508, MIL-HDBK-29612). Courses currently planned for development/improvement, along with their expected date of completion, include the following:

- CFATS Course for New Inspectors (FY13)
- AUO Training (FY13)
- Risk Based Performance Standard 8 – Cyber Security Inspections (FY13)
- Regulatory / Compliance Review training courses for all ISCD personnel (FY14)
- Basic level trainings specific to various job series (FY14)
- Updated training on Federal, State, local and private sector outreach (FY14)
- Advanced level trainings specific to various job series (FY15)
- Training on Ammonium Nitrate for Inspectors and other selected personnel (TBD based on timing of issuance of Ammonium Nitrate Security Program final rule)

Recommendation 10: Develop and implement program metrics that measure CFATS Program value accurately and demonstrate the extent to which risk has been reduced at regulated facilities.

Response: Concur/Completed. During FY 2012, the ISCD Program Management Office developed an Annual Operating Plan (AOP) containing CFATS program performance metrics for FY13 and beyond, including defined milestones, performance measures, and data points that will be tracked to monitor program performance. The subject listings are extensive and cover the full gamut of CFATS program execution including business support activities. The AOP is an ISCD Director approved document. The performance metrics recognize both current and projected measurement start dates as some business processes do not start until FY14 or later. As of the first quarter of FY13, there are 38 listed milestones, 73 performance measures, and 73 key data tracking elements. These measures are subject to quarterly reviews and updates.

Additionally, ISCD recently updated its Government Performance and Results Act (GPRA) metric to better reflect program progress. Specifically, the CFATS program developed a performance measure based on its Risk-Based Performance Standards (RBPS) with defined fiscal year (FY) performance targets that measure the degree of covered facilities' compliance with the CFATS regulation. The new GPRA measure tracks and reports on the percentage of applicable RBPS that are confirmed through the SSP/ASP approval process as having been met by Tier 1 and Tier 2 covered facilities. Tier 3 and Tier 4 targets are planned to be defined in late FY13. This performance measure is reflective of the CFATS regulation's value and impact on regulated facilities' risk reduction. This measure has been approved as the reporting metric for GPRA by both DHS leadership and the White House's Office of Management and Budget.

Recommendation 11: Develop a strategy and implement a plan to work with Congress and private industry to ensure long-term authorization for the CFATS Program.

Response: Concur. The long-term authorization of CFATS remains a top priority for NPPD. Over the past few months, ISCD has worked closely with the DHS Office of Legislative Affairs (OLA) to proactively engage Congress and reinforce the message that long-term authorization is a Departmental priority. The Department has advocated for long term reauthorization in congressional testimony and has worked with our interagency partners to ensure that Congress receives a consistent message. Additionally, NPPD stands ready to provide whatever technical assistance or other input Congressional members request in regards to CFATS reauthorization.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Perhaps most importantly, as described above, ISCD has significantly increased the pace at which it is reviewing, authorizing, inspecting, and approving SSPs; recently approved its first Alternative Security Programs (ASP); successfully assisted an industry association's efforts to develop an ASP template for use by its members; engaged industry in ways to improve the information technology systems supporting the implementation of CFATS; and achieved a number of other programmatic successes and milestones. NPPD leadership believes there is nothing more critical to achieving long-term authorization of CFATS than the successful implementation of CFATS and recognition that the program is headed in the right direction. NPPD leadership is proactively sharing these success stories with members of Congress.

Recommendation 12: Develop a methodology and reporting process to identify and address errors and anomalies that arise in the CFATS tiering methodology and risk engine.

Response: Concur. Even though the anomalies occurred only with the tiering of sabotage and release chemicals of interest, which accounts for less than 15 percent of the CFATS regulated community, ISCD is undertaking a three-phased approach to review the tiering process. This three-phased approach, which is reflected in Action Item 94 of ISCD's current Action Plan, includes the following activities:

1. Thoroughly document all processes and procedures relating to the tiering methodology;
2. Conduct an internal DHS review of the complete tiering process; and
3. Conduct an external peer review of the risk-based tiering methodology.

The first two phases were completed by NPPD in 2012 while the OIG review was underway. The third item, the external peer review, began in January 2013. It is being led by a non-profit Federally Funded Research and Development Center and involves experts from Government, industry, and academia. The peer review panel has been tasked with reviewing the existing CFATS risk methodology to see if it is a justifiable and reasonable approach for tiering high risk chemical facilities. While the peer review has the ability to look at any and all aspects of the existing risk methodology, the Department did provide the peer review panel with a list of potential areas for improvement that the Department identified in the first two phases of its three-phased review of the risk methodology. The results of the peer review are expected to be provided to the Department in the third quarter of FY 2013.

In addition to this formal review, the SVA and SSP review processes have been developed in a manner that requires multiple subject matter expert (SME) reviews of facility submissions. If at any point in time an SME identifies a potential anomaly in a facility's tiering, that anomaly is investigated to determine if it was a facility data error, an error within the tiering engine or risk methodology, or not an anomaly at all. This supports a continuous improvement process which ISCD has in place for all of its processes and methodologies.

Recommendation 13: Provide the external peer review results, including comments on the V Factor, and ISCD's action plan to implement external peer review recommendations.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Response: Partially Concur. While ISCD supports the notion of acting appropriately on the external peer review findings and would be pleased to share those findings with the appropriate entities, it is unclear with whom the OIG is recommending ISCD share those results. Given the lack of clarity, NPPD cannot concur in full with the recommendation. In addition, while all recommendations from the peer review will be considered, the Department cannot commit to implementation of the recommendations until the Department knows what the recommendations are. It should also be noted that the CFATS risk methodology's treatment of vulnerability (i.e., the "V Factor") is one of the specific areas that ISCD informed the peer review panel ISCD is particularly interested in receiving feedback from the peer review panel on.

Recommendation 14: Reduce overall ISCD reliance on contract personnel to avoid the appearance that contractors may be performing inherently governmental functions and closely associated governmental functions.

Response: Non-Concur. To ensure that ISCD has the appropriate mix of Federal and contractor skills, expertise, experience, and other assets necessary to effectively achieve the Department's mission, each new and re-competed contract is analyzed utilizing the DHS Balanced Workforce Strategy tool to assess risk, ability to provide adequate oversight, and cost. Based on the analyses done to date, we do not believe that ISCD is overly reliant on contract personnel, nor do we believe that any contractors are performing inherently governmental functions or inappropriately performing closely associated governmental functions (which, the OIG Report fails to note, contractors are allowed to perform so long as they do so with proper supervision by a Federal employee).

NPPD also notes that there is no substantiating evidence for any of the allegations made by the OIG regarding contractors performing inherently governmental functions, nor any specific examples of activities that give the perception of such prohibited activity. Nevertheless, ISCD, in conjunction with NPPD Finance, will perform an assessment of ISCD's current level of contract personnel to confirm that there is not an overreliance on contract personnel. Additionally, NPPD and ISCD will continue to review all new ISCD procurements under the DHS Balanced Workforce Strategy to ensure the Scopes of Work for contractors do not include any inherently governmental functions.

Recommendation 15: Develop and implement a learning curriculum that (1) describes position roles and responsibilities clearly; (2) provides comprehensive training plans to prepare employees to perform assigned duties; and (3) communicates measures to assess performance.

Response: Concur. In 2012, ISCD conducted human resources planning to determine and identify the human resources and the necessary skill sets required for program success. Based on these activities, ISCD realigned its organization on a functional basis and clarified functional unit roles and responsibilities. Using this and other information as a baseline, ISCD is developing a Human Resource Plan which will include a staffing management plan and identification of training needs for all staff. ISCD is utilizing a workforce analysis methodology to complete this Human Resources Plan. This workforce analysis will include:

- Conducting a job analysis for each position;
- Creating new/revised position descriptions and job/task analysis worksheets for each position;



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Identifying required skills and competencies for each job;
- Creating new performance plans and standards by job; and
- Implementing new Individual Developmental Training plans targeted at developing and/or maintaining required skills and competencies.

Following the completion of the Human Resources Plan, ISCD intends to develop and disseminate an ISCD Employee Handbook that describes for all staff various aspects of the Human Resources Plan.

Recommendation 16: Develop NPPD-wide policy regarding appointment of acting management in accordance with Office of Personnel Management guidelines.

Response: Concur/Completed. NPPD already has developed and issued an NPPD Merit Promotion Plan that states requirements for details and temporary promotions that are consistent with OPM requirements. To ensure that NPPD managers and human capital staff at all levels of NPPD understand the policies surrounding the appointment of acting management, NPPD Human Capital intends to provide training on the topic to appropriate individuals.

Recommendation 17: Ensure that all employees serving in an acting supervisory capacity have a supervisory position description in accordance with Office of Personnel Management requirements.

Response: Non-Concur. The term “acting” does not have a formal definition under Office of Personnel Management (OPM) guidelines nor does OPM require that employees performing supervisory duties in an “acting” capacity always have a supervisory position description. The term “acting” may be used to cover anything from full assumption of duties of a position, to temporarily covering one-day absences, to serving as a point-of-contact but not covering all aspects of the position. However, it is important that managers are diligent in applying the rules for details when temporarily assigning employees to other duties. To alleviate any misunderstanding, we are exploring developing Human Resources (HR) training for managers that specifically address these topics.

Recommendation 18: Ensure that all employees receive performance reviews according to NPPD’s General Instruction Guide on performance management.

Response: Concur. On December 31, 2012, NPPD’s Employee and Labor Relations Office issued a memorandum on Performance Management guidance that requires all non-SES employees to receive at least one formal documented progress review throughout the performance cycle. A signed acknowledgement form, to include feedback from the supervisor, is to be provided to the employee. This memo also addressed a new requirement for the subcomponent Chiefs of Staff to document and validate dates each employee signed a progress review by utilizing the NPPD Performance Plan and Appraisal Report Certification (PPARC). This report is to be submitted to NPPD for progress reviews by March 15, 2013, and close-out reviews with summary ratings by August 9, 2013. Due to the new requirements implemented by NPPD, ISCD is on track to ensure all employees receive both a mid-year and a close-out review, which will ensure that supervisors actively engage with employees on their progress throughout



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

the performance cycle. Going forward, ISCD intends to use the PPARC to track ISCD's completion of all required performance reviews.

Recommendation 19: Eliminate the authorization and payment of Administratively Uncontrollable Overtime for all ISCD personnel.

Response: Non-Concur. While NPPD acknowledges that there previously were some issues related to the application and management of AUO within ISCD, these issues are being addressed. Moreover, based on the findings of an internal audit of the ISCD AUO program, there are legitimate justifications supporting the use of AUO by ISCD Chemical Security Inspectors. Based on that audit, ISCD leadership has determined that the more appropriate path regarding AUO for ISCD Chemical Security Inspectors is to continue to permit AUO in a manner that evolves consistently with AUO rules and regulations, and that is supported by greater oversight, increased training, documented policies and procedures, and greater management controls. Pertinent details on the ISCD audit and other AUO related developments are provided below.

In May 2012, ISCD initiated a follow-on audit to look in greater detail at ISCD's management of AUO, including, among other things, an examination of what each AUO-authorized individual claimed as AUO, what percentage of those claims were and were not justified under AUO regulations, what management controls regarding AUO were in place, and what improvements could be made by ISCD to better manage AUO. To better ensure that all components within NPPD follow proper AUO protocols, in September 2012, NPPD issued an NPPD AUO Instruction, which established policies and procedures for the approval, certification, and payment of AUO. That document requires all employees occupying positions that have been approved for AUO, as well as the supervisors of those employees, complete training on AUO regulations, policies, roles and responsibilities. The NPPD Human Capital Office monitors the training to ensure that all affected employees have completed it. The guidance also requires that certifying officials review all AUO authorized position descriptions to ensure that the work assigned to the employee is expected to meet the requirements for payment of AUO premium pay. Certifying officials must review the accuracy of and approve/disapprove weekly AUO reports for each employee, and four times each year, they must review the time and attendance and related records for all employees receiving AUO premium pay to ensure they meet the requirements for payment of the rates authorized and make adjustments when necessary. Records of these reviews are to be maintained by certifying officials/first-line supervisors of employees receiving AUO for six years and be available for review and/or inspection. Under that policy, NPPD is in the process of conducting a review to ensure that all positions within NPPD for which AUO is currently being claimed are appropriate for AUO.

Additionally, ISCD has recently completed draft Division-level AUO guidance to expand on the guidance provided by NPPD. This draft guidance will enumerate specific CFATS-related activities that are and are not AUO eligible and will describe and detail the frequency of both supervisory reviews and formal audits (i.e., Periodic Reviews). This draft guidance is anticipated to be completed and signed by ISCD leadership by the end of April 2013.

Recommendation 20: Establish internal controls to ensure accountability for all ISCD appropriated funds and that sufficient justification exists for all procurements.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Response: Concur/Completed. ISCD has established several internal controls and approval forms in order to ensure appropriate funding accountability. Within the AOP, ISCD has established metrics that allow for ISCD leadership to see quarterly updates on the Division's progress towards meeting this accountability objective. As the owner of the AOP, the ISCD Program Management Office has developed formal objectives to help ensure the appropriated funds are accounted for and expended as necessary. ISCD works to ensure less than or equal to a 10 percent variance between appropriated funding and obligated funding within the current fiscal year. Working under one year funds, ISCD ensures procurements are executed as planned and within the funding limits. The procurement administrative lead timelines (PALT) are also tracked, and ISCD works to achieve a 95 percent or higher completion rate of procurements within the Office of Procurement Operations PALT guidelines.

ISCD also recently implemented an Acquisition Justification Form to be used internally for funding requests for approval. The form includes requirement descriptions, funding amounts, and mitigation strategies in the event of disapproval. The form ensures execution alignment with the ISCD fiscal year spendplan in coordination with IP. The spendplan is a tracking mechanism for the Division as well as IP to properly fund each quarter based on requirement needs.

Contractor performance and fund expenditure rates are closely monitored via cost and schedule reports, and periodic project and technical management reviews. In addition, billing submissions are scrutinized and planned performance objectives are compared with actual results.

Recommendation 21: Advertise and select permanent ISCD leadership with demonstrated qualifications and skills at all levels, to include Division Director, Deputy Division Director, branch chiefs, deputy branch chiefs, and section chiefs.

Response: Concur. NPPD agrees that having a permanent, qualified ISCD leadership team is critical to the long-term success of the CFATS program, and we collectively have been diligently working towards that end over the past few months. ISCD has filled or is in the process of filling all ISCD leadership positions with permanent, qualified individuals. ISCD currently has a permanent Director, Deputy Director and Chief of Staff. Of the five Branch Chief positions in ISCD, one is filled, two additional individuals have accepted permanent offers and will be moving in to those positions in the near future, and selections will soon be made for the remaining two positions. Of the five Deputy Branch Chief positions, one is filled and the interviews are being scheduled or have been completed for the other four positions. Eight of the twelve Section Chief positions are filled with permanent Section Chiefs, two additional individuals have accepted offers to be permanent Section Chiefs, and interviews are being scheduled for the final two Section Chief positions. In regard to field leadership positions, all but two of the thirteen District and Regional Commander positions are filled with permanent leadership, and the vacancy announcement for the remaining two positions closed on February 5, 2013.

Recommendation 22: Develop and disseminate an ISCD organizational and reporting structure to all ISCD staff.

Response: Concur/Completed. On January 14, 2013, the ISCD Director disseminated an ISCD organizational chart to all ISCD staff that included the ISCD reporting structure.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation 23: Reiterate to all NPPD employees the process for reporting misconduct allegations.

Response: Concur/Completed. On January 16, 2013, NPPD Under Secretary Beers disseminated a message to all NPPD employees announcing the implementation of the Principles of Integrity and Professional Responsibility Management Directive. Included in that message were the reporting procedures for employees to submit allegations of misconduct. Additionally, the NPPD Office of Compliance and Security (OCS) has updated its web site to include the proper procedures and contact information for reporting allegations of misconduct. NPPD intends to continue to regularly reiterate the reporting procedures to its employees and NPPD OCS is working with the Public Affairs Office to draft an updated memorandum or message to all employees.

Recommendation 24: Improve the clarity of guidance provided to the CFATS-regulated industry so that it can benefit from regular and timely comments on facility submissions.

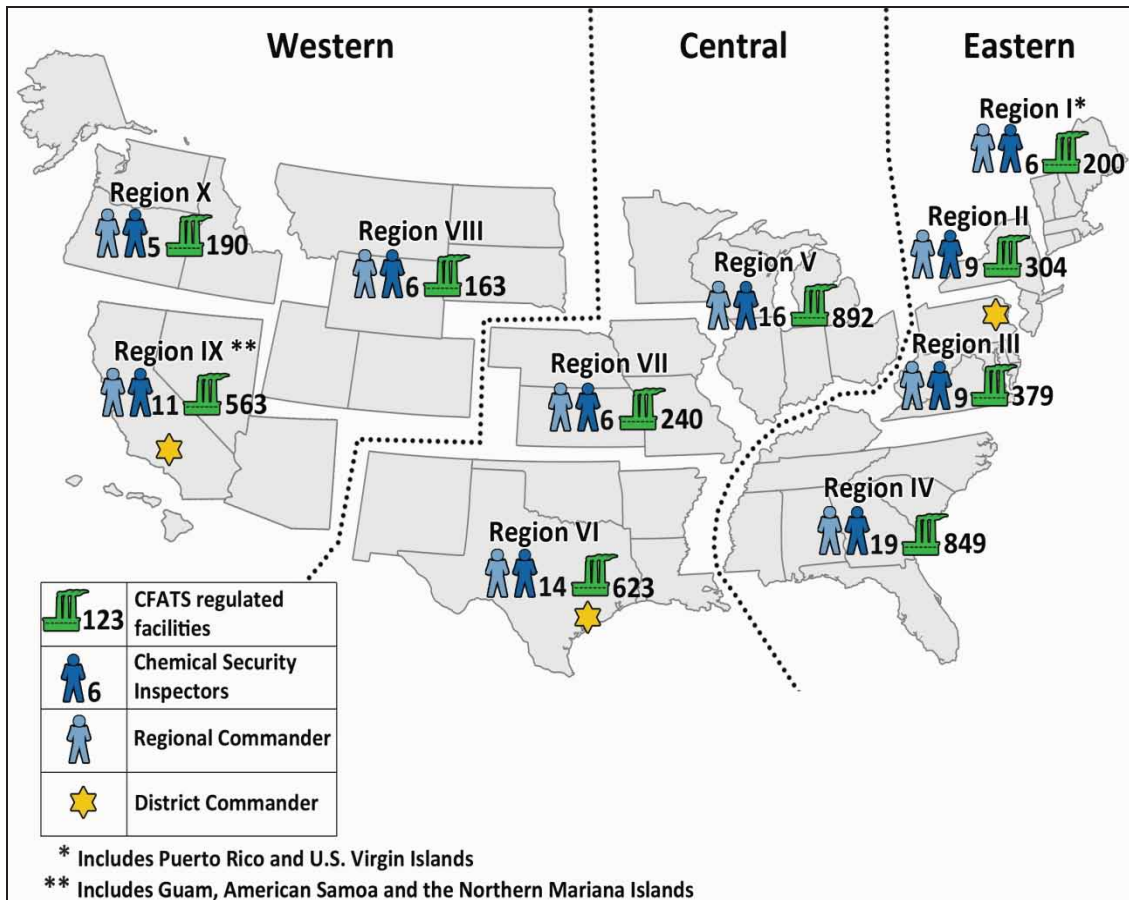
Response: Concur. As part of its efforts to improve the Chemical Security Assessment Tool, ISCD intends to update its guidance materials for the Top-Screen, SVA, and SSP. ISCD is also in the process of developing updated guidance related to its Chemical-terrorism Vulnerability Information program, and intends to release guidance specific to the CFATS Personnel Surety Program when the CFATS Personnel Surety Program is launched. Finally, ISCD intends to routinely update its website and Frequently Asked Questions page based on user feedback in order to provide clear guidance and assistance to the regulated community.

Sincerely,

Rand Beers
Under Secretary



Appendix D ISCD Field locations, Staff, and Regulated Facilities



Source: OIG analysis as of October 23, 2012.



Appendix E

F1 Factor Timeline of Events

Date	Activity
May 2009	ISCD begins issuing final tier assignments
December 2009	Anomalies observed in final facility tier determinations
January 2010	Initial F1 Factor error identified
May 25, 2010	ISCD leadership observed anomalies in the May 2010 tiering run of facilities and requested that staff review the issue
May 27, 2010	ISCD subject matter experts developed an action plan to address F1 Factor problem and briefed ISCD leadership
May 28, 2010	ISCD leadership emailed IP leadership regarding the postponement of the May 2010 tier notification letters
June 2010	National laboratories' report on F1 Factor delivered to ISCD
June 18, 2010	Tier notification letters mailed to facilities; ISCD leadership informs IP leadership and NPPD representatives
November to December 2010	ISCD subject matter experts identified inconsistencies in tiering levels in the review of Tier 1 SSP redeterminations
January 25, 2011	ISCD subject matter experts brief new ISCD leadership about the unresolved F1 Factor problem
February 4, 2011	ISCD subject matter experts notify ISCD leadership of number of affected facilities; ISCD leadership notifies IP leadership
February to March 2011	ISCD leadership convenes F1 Factor problem working group
April 8, 2011	ISCD receives results of tiering run with correct F1 Factors for facilities tiered before June 2010
May 2011	ISCD F1 Factor problem working group finalizes and presents recommendations to ISCD leadership
June 1, 2011	ISCD leadership informs IP leadership of findings
June 2, 2011	IP leadership briefs NPPD's Under Secretary
June 27, 2011	ISCD contacted the affected facilities in writing to advise them of a revision to the original SVA risk engine data
June 28, 2011	IP leadership misconduct allegation to DHS OIG, noting the failure of IP officials to provide timely and sufficient notification
June 30, 2011	Blog posting regarding rumored retiering notification letters sent to approximately 400 CFATS-covered facilities
July 5, 2011	Statement on DHS website on revised tier assignments
October 1, 2011	OCS assigned investigation to one of its senior special agents

Source: OIG analysis.



Appendix F

F1 Communication to IP leadership and NPPD Staff

Sent: Fri May 28 09:39:01 2010

Subject: CFATS May Tier Notification -- DELAY TO JUNE

All,

For your information, I have decided not to move forward with the 425+ facility batch of final tier notification for May which was previously scheduled to go out today.

This batch is focused on preliminary tier 4 release-toxic facilities and we are seeing some unexpected results. ISCD will take 1-2 weeks to analyze & understand what we are seeing and why, and push forward from there.

Longer term, the path forward from here is to issue a June tier notification batch (prior to or in conjunction with the Chemical Security Summit), then a late July batch, and then an August batch. This will still allow us to meet our commitment for completing all final tiering by end of Summer 2010.

I'll keep you posted. I am not advising the Sector Coordinating Council and do not think this requires congressional notification. Let me know if you have a differing opinion.

Sent: Friday, June 18, 2010 12:14 PM

Subject: FW: CFATS June Tier Notification Batch

I wanted to send a quick follow-up note regarding the May tier notification (or lack thereof). We figured out that the May tier notification batch (tier 4 release toxic facilities) had *test data* rather than *real data* in the geospatial population calculation algorithm ("F1"). This caused the numbers to skew. We use test data to ensure the tools are working properly, ironically. This has not been a problem in the past (this was the first batch of *tier 4* release toxic facilities) and the problem was relatively easy to fix once identified. We just had to take the time to find which factor was off and why.

Source: ISCD program files.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix G

Designation of Leadership Positions in IP

*Office of Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528*



**Homeland
Security**

MEMORANDUM FOR: IP Division Directors
IP Deputy Division Directors
IP Employees

FROM: [REDACTED] 20090917
Deputy Assistant Secretary

SUBJECT: Designation of Leadership Positions in the Office of Infrastructure Protection (IP)

As a follow-on to the designation of [REDACTED] as the Acting Assistant Secretary (ASIP) and [REDACTED] as the Acting Deputy Assistant Secretary (DAS), I am pleased to announce additional leadership designations within the Office of Infrastructure Protection that will ensure team continuity and mission focus during this period of transition.

While [REDACTED] is handling the responsibilities of Acting ASIP, [REDACTED] is designated as the Acting Division Director for the Protective Security Coordination Division. While [REDACTED] is the Acting Division Director, [REDACTED] is designated as the Deputy Division Director.

While [REDACTED] is handling the responsibilities of Acting DAS, [REDACTED] is designated as the Acting Division Director for the Infrastructure Security Compliance Division. While [REDACTED] is the Acting Division Director, [REDACTED] is designated as the Deputy Division Director.

While [REDACTED] is attending the National Defense University, [REDACTED] is designated as the Acting Division Director for the Contingency Planning Incident Management Division. While [REDACTED] is the Acting Division Director, [REDACTED] is designated as the Deputy Division Director.

Please join me in congratulating all these individuals in their new responsibilities. I ask that you give these IP leaders your full support as we continue our mission to strengthen the security and resiliency of our Nation's Critical Infrastructure and Key Resources.

Source: ISCD program files.



Appendix H

Major Contributors to This Report

Marcia Moxey Hodges, Chief Inspector

Angela Garvin, Lead Inspector

Katherine Yutzey, Senior Inspector

Amy Tomlinson, Inspector

Adam C. Brown, Inspector

Matthew Salaga, Inspector



Appendix I

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
Acting General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
NPPD Audit Liaison
IP Audit Liaison
Director of Local Affairs, Office of Intergovernmental Affairs
Acting Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate
Chairman, House Committee on Homeland Security, Subcommittee on Cybersecurity,
Infrastructure Protection and Security Technologies
Ranking Member, House Committee on Energy and Commerce

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.