United States Government Accountability Office

Report to Congressional Committees

June 2017

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Fully Implemented Its Chemical Security Expedited Approval Program, and Participation to Date Has Been Limited

GAO-17-502

June 2017

CRITICAL INFRASTRUCTURE PROTECTION

DHS Has Fully Implemented Its Chemical Security Expedited Approval Program, and Participation to Date Has Been Limited

GAO Highlights

Highlights of GAO-17-502, a report to congressional committees

Why GAO Did This Study

Facilities that produce, use, or store hazardous chemicals could be of interest to terrorists intent on using them to inflict mass casualties in the United States. DHS established the CFATS program to, among other things, identify and assess the security risk posed by chemical facilities. DHS places high-risk facilities into one of four risk-based tiers and inspects them to ensure compliance with DHS standards. The CFATS Act of 2014 created the Expedited Approval Program as an option for the two lower-risk tier facilities (tiers 3 and 4) to reduce the burden and expedite the processing of security plans. The act further required that DHS report on its evaluation of the expedited program to Congress.

The CFATS Act of 2014 also included a provision for GAO to assess the expedited program. This report discusses (1) DHS's implementation of the expedited program and its report to Congress and (2) the number of facilities that have used the program and factors affecting participation in it. GAO reviewed laws and DHS guidance, analyzed DHS's report to Congress, and interviewed DHS officials. GAO also received input from officials with three industry groups that represented the most likely candidates to use the program, and officials representing eight of their member organizations. The results of this input are not generalizable, but provide insights about the expedited program.

GAO is not making recommendations in this report.

View GAO-17-502. For more information, contact Chris Currie at (404) 679-1875 or CurrieC@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) fully implemented the Chemical Facility Anti-Terrorism Standards (CFATS) Expedited Approval Program in June 2015 and reported to Congress on the program in August 2016, as required by the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (CFATS Act of 2014). DHS's expedited program guidance identifies specific security measures that eligible (i.e., tiers 3 and 4) high-risk facilities can use to develop expedited security plans, rather than developing standard (non-expedited) security plans. Standard plans provide more flexibility in securing a facility, but are also more time-consuming to process. DHS's report to Congress on the expedited program discussed all required elements. For example, DHS was required to assess the impact of the expedited program on facility security. DHS reported that it was difficult to assess the impact of the program on security because only one facility had used it at the time of the report. DHS officials stated that they would further evaluate the impact of the program on security if enough additional facilities use it in the future.

As of April 2017, only 2 of the 2,496 eligible facilities opted to use the Expedited Approval Program; various factors affected participation. Officials from the two facilities told GAO they used the program because its prescriptive nature helped them quickly determine what they needed to do to implement required security measures and reduced the time and cost to prepare and submit their security plans to DHS. According to DHS and industry officials GAO interviewed, low participation to date could be due to several factors:

- DHS implemented the expedited program after most eligible facilities already submitted standard (non-expedited) security plans to DHS;
- the expedited program's security measures may be too strict and prescriptive, not providing facilities the flexibility of the standard process; and
- DHS conducts in-person authorization inspections to confirm that security plans address risks under the standard process, but does not conduct them under the expedited program. DHS officials noted that some facilities may prefer having this inspection because it provides them useful information.

Recent changes in the CFATS program could also affect future use of the expedited program. In fall 2016, DHS updated its online tool for gathering data from facilities. Officials at DHS and 5 of the 11 industry organizations GAO contacted stated that the revised tool is more user-friendly and less burdensome than the previous one; however, it is unclear how the new tool might affect future use of the expedited program. Also, in fall 2016, DHS revised its methodology for determining the level of facility risk, and one of the two facilities that participated in the expedited program is no longer deemed high risk. DHS is continuing to apply the methodology to other facilities regulated under the CFATS program; therefore, it is too early to assess the impact on participation.

Contents

Abbreviations:

CFATS	Chemical Facility Anti-Terrorism Standards
DHS	Department of Homeland Security
EAP	Expedited Approval Program
ISCD	Infrastructure Security Compliance Division

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 29, 2017

Congressional Committees

The United States has hundreds of thousands of facilities that produce, use, or store hazardous chemicals that could be used by terrorists to inflict mass casualties and damage. These chemicals could be released from a facility to cause harm to surrounding populations, stolen and used as chemical weapons, or stolen and used to build an improvised explosive device.

The Chemical Facility Anti-Terrorism Standards (CFATS) program—initially established pursuant to the Department of Homeland Security (DHS) Appropriations Act, 2007—enables DHS to, among other things, identify chemical facilities and assess the security risk posed by each, categorize the facilities into risk-based tiers, and inspect the high-risk facilities to ensure compliance with regulatory requirements.[1] The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (CFATS Act of 2014), enacted in December 2014, in effect, reauthorized the CFATS program for an additional 4 years while also imposing additional implementation requirements on DHS for the program.[2] We previously reported on various aspects of the CFATS program and made a number of recommendations in recent years to strengthen the program. DHS agreed with all of these recommendations and has either fully implemented or taken action to address them.[3]

[1]See 72 Fed. Reg. 17,792 (Apr. 9, 2007) (interim final rule) (codified as amended at 6 C.F.R. pt. 27); see also Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388-89 (2006).

[2]See Pub. L. No. 113-254, 128 Stat. 2898 (2014); 6 U.S.C. §§ 621-29. Specifically, the Act amended the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), as amended, by adding Title XXI—Chemical Facility Anti-Terrorism Standards—and expressly repealed the program's authority under the fiscal year 2007 DHS appropriations act.

[3]GAO, *Critical Infrastructure Protection: DHS Is Taking Action to Better Manage Its Chemical Security Program, but It Is Too Early to Assess Results*, GAO-12-515T (Washington, D.C.: July 26, 2012); *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, GAO-13-353 (Washington, D.C.: Apr. 5, 2013); *Critical Infrastructure Protection: DHS Action Needed to Verify Some Chemical Facility Information and Manage Compliance Process*, GAO-15-614 (Washington, D.C.: July 22, 2015); and *Critical Infrastructure Protection: Improvements Needed for DHS's Chemical Facility Whistleblower Report Process*, GAO-16-572 (Washington, D.C.: July 12, 2016).

DHS's National Protection and Programs Directorate's Infrastructure Security Compliance Division (ISCD) manages the CFATS program. DHS assigns high-risk facilities to one of four risk tiers, where tier 1 represents facilities with the highest risk and tier 4 represents facilities with the lowest risk. As of September 2016, DHS had designated 2,947 facilities in the United States as high risk and assigned to a tier. Once a facility is assigned to a tier, it is required to develop a site security plan and submit it to DHS. The security plan describes how a facility's existing and planned security measures address applicable Risk-Based Performance Standards —18 standards that identify areas of a facility's security posture that are to be examined, such as perimeter security, access control, and cybersecurity.[4] The CFATS program also provides high-risk facilities the option of submitting an Alternative Security Program in place of the site security plan.[5]

Members of Congress and the chemical sector have expressed concern about the administrative burden associated with the development of facility security plans and the pace of DHS efforts to process and approve them. In response to this concern, the CFATS Act of 2014 created an Expedited Approval Program (EAP) as another option that tier 3 and tier 4 facilities may use to develop and submit security plans to DHS.[6] Unlike the standard CFATS process in which facilities decide how to meet Risk-

[4]See 6 C.F.R. § 27.230. According to ISCD, planned security measures are in the process of being implemented by a facility that can be assessed by DHS to determine if a facility's site security plan satisfies applicable Risk-Based Performance Standards. Planned security measures include those in the design phase that have an approved and documented capital budget, in the bid process that have been placed for bid or have been received and are under review, and in a pilot phase or in execution as a demonstration project that have a documented implementation budget and schedule. Examples of 2 of the 18 Risk-Based Performance Standards are: (1) Restrict Area Perimeter - secure and monitor the perimeter of the facility, and (2) Secure Site Assets - secure and monitor restricted areas or potentially critical targets within the facility. To meet Risk-Based Performance Standards, facilities may choose the security programs or processes they deem appropriate to address the performance standards as long as ISCD determines that the facilities achieve the requisite level of performance on each applicable area in their existing and agreed-upon planned measures.

[5]An Alternative Security Program is a third-party or industry organization program; a local authority, state, or federal government program; or any element or aspect thereof that has been determined to meet the requirements of, and provide for an equivalent level of security to that established by, the CFATS regulation. See 6 C.F.R. § 27.105. DHS may approve an Alternative Security Program, subject to revisions or supplements, if it meets the requirements of the CFATS rule and satisfies all applicable Risk-Based Performance Standards.

[6]See Pub. L. No. 113-254, § 2(a), 128 Stat. at 2901 (codified at 6 U.S.C. § 622(c)(4)).

Based Performance Standards, the EAP prescribes specific security measures that facilities must have in order to meet the standards. According to committee report language, the EAP is expected to reduce the time and burden on smaller chemical companies, which may lack the compliance infrastructure and resources of large chemical facilities.[7] The act also required DHS to assess the expedited program and report to Congress.

The CFATS Act of 2014 also included a provision for GAO to examine DHS's implementation of the EAP and DHS's report on the program.[8] This report discusses: (1) DHS's implementation of the EAP and assessment of the program in its report to Congress and (2) the number of facilities that have used the EAP and factors affecting participation in the program.

To address our first objective, we reviewed the *DHS Guidance for the Expedited Approval Program* (EAP guidance) and documentation about the process ISCD uses to vet site security plans under the EAP, security plans under the standard (i.e., non-expedited) CFATS process, and Alternative Security Programs.[9] We also interviewed senior ISCD officials about their process for developing the EAP guidance and reviewing submissions. To obtain insight into how ISCD developed the guidance, we selected 10 of the 157 security measures from the EAP guidance to reflect variation in the types of security measures and asked ISCD officials to explain how they developed each measure and why they

[7]S. Rep. No. 113-263, at 9 (Sept. 18, 2014).

[8]See Pub. L. No. 113-254, § 3(c)(2)(D), 128 Stat. at 2918 (2014).

[9]DHS, *DHS Guidance for the Expedited Approval Program* (Washington, D.C.: May 12, 2015).

required each measure.[10] In addition, we reviewed the CFATS Act of 2014 to identify the EAP elements that the act requires DHS to assess and report to Congress.[11] We compared the DHS report with the required elements in the CFATS Act of 2014 to determine the extent to which DHS's report discussed each element listed in the statute.[12]

To address our second objective, we reviewed ISCD data on EAP-eligible (i.e., all tier 3 and tier 4) facilities before and after ISCD implemented the EAP in June 2015, and calculated the number and percentage of EAP-eligible facilities that already had approved security plans and Alternative Security Programs under the standard CFATS process before and after ISCD implemented the EAP. To assess the reliability of ISCD data, we reviewed interviews and documentation that we previously collected for our 2015 report on the CFATS program and questioned ISCD officials about the extent that ISCD's processes and procedures for tracking the number of tier 3 and tier 4 facilities have changed since 2015.[13] We determined the data to be sufficiently reliable for our purposes. We also reviewed the site security plans submitted by the two facilities that used the EAP as of April 2017, in order to identify characteristics about the facilities and their security measures.[14] In addition, we reviewed ISCD

[10]To select the 10 EAP security measures, we selected two required security measures from each of the five security measure sections in DHS's EAP guidance document: detection measures, delay measures, response measures, cyber security measures, and security management measures. We also assigned all security measures in the guidance to three broad categories and selected at least two security measures from each of three broad categories. To determine these categories, we reviewed each measure in the guidance and identified the broad categories to which the measures generally belonged. We found that some measures belonged in multiple categories. The categories we identified are: physical or technological specifications, security process or procedures, and security management or administration. We selected the 10 security measures to reflect a variety of these categories. To the extent possible, we chose measures that were very prescriptive in nature. For example, we selected one security measure because it prescribes, among other things, the types of material a facility must use if it chooses to employ fences or walls and the specific heights that the fences and walls must be for them to meet Risk-Based Performance Standards.

[11]See 6 U.S.C. § 622(c)(4)(I)(2).

[12]DHS, *Chemical Facility Anti-Terrorism Standards Expedited Approval Program Report* (Washington, D.C.: Aug. 2, 2016).

[13]GAO-15-614.

[14]On April 7, 2017, an ISCD official notified us that one of the two facilities that had used the EAP was no longer considered to be high risk and, therefore, was no longer an EAP facility.

documentation, such as e-mails between the facilities that used the EAP and ISCD, and interviewed officials from the two facilities that participated in the EAP to obtain their perspectives, including why they chose to use the EAP.

Furthermore, we interviewed ISCD officials who review expedited security plans to identify and examine factors that affected the use of the EAP. In addition, we selected industry officials and obtained their perspectives, including ISCD's communication with them about the EAP and factors that affect facility officials' use of it. In so doing, we interviewed officials in 11 industry organizations. Specifically, we interviewed the Chairs and Vice Chairs of the Chemical Sector Coordinating Council, Food and Agriculture Sector Coordinating Council, and the Oil and Natural Gas Subsector Coordinating Council of the Energy Sector Coordinating Council, that ISCD officials told us they informed about the EAP and its availability for use.[15] According to ISCD officials, facilities in these sectors and subsectors would be the most likely candidates to use the EAP. We also selected eight member organizations (for example, trade associations or companies)—four member organizations for the Chemical Sector Coordinating Council, three member organizations for the Oil and Natural Gas Subsector Coordinating Council, and one member organization for the Food and Agriculture Sector Coordinating Council—and interviewed key officials in those organizations about the EAP.[16] The results of these interviews are not generalizable, but they provide insights about the EAP.

[15]Sector Coordinating Councils are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. For example, the Chemical Sector Coordinating Council represents owners and operators of chemical facilities. The Sector Coordinating Councils coordinate and collaborate with sector-specific agencies and related Government Coordinating Councils to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.

[16]We selected three member organizations to interview by asking Sector Coordinating Council and Subsector Coordinating Council Chairs and Vice Chairs to recommend member organizations that the Chairs and Vice Chairs thought may be eligible for and knowledgeable about the EAP. We selected three member organizations by identifying them from interviews conducted for one of our prior reports on the CFATS program and by researching information about them on the internet. We selected two member organizations by asking ISCD to recommend member organizations that have members eligible to use the EAP.

We conducted this performance audit from August 2016 to June 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DHS's National Protection and Programs Directorate leads the country's effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. The directorate includes the Office of Infrastructure Protection, which leads the coordinated national effort to reduce risk to U.S. critical infrastructure posed by acts of terrorism. Within the Office of Infrastructure Protection, ISCD leads the nation's effort to secure high-risk chemical facilities and prevent the use of certain chemicals in a terrorist act on the homeland; ISCD also is responsible for implementing and managing the CFATS program, including its EAP.

The CFATS program is intended to ensure the security of the nation's chemical infrastructure by identifying, assessing the risk posed by, and requiring the implementation of measures to protect high-risk chemical facilities. Section 550 of the DHS Appropriations Act, 2007, required DHS to issue regulations establishing Risk-Based Performance Standards for chemical facilities that, as determined by DHS, present high levels of risk; the act also required vulnerability assessments and development and implementation of site security plans for such facilities.[17] DHS published the CFATS interim final rule in April 2007 and appendix A to the rule, published in November 2007, lists 322 chemicals of interest and the screening threshold quantities for each.[18] According to DHS, subject to certain statutory exclusions, all facilities that manufacture chemicals of interest, as well as facilities that store or use such chemicals as part of

[17]Pub. L. No. 109-295, § 550, 120 Stat. at 1388-89.

[18]72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified as amended at 6 C.F.R. pt. 27); 72 Fed. Reg. 65,396 (Nov. 20, 2007) (codified at 6 C.F.R. pt. 27, App. A). The interim final rule (i.e., the CFATS regulation), as subsequently amended, remains in effect. Appendix A has not been revised since its initial publication.

their daily operations, may be subject to CFATS.[19] However, only chemical facilities determined to possess a requisite quantity of chemicals of interest (i.e., the screening threshold quantity) and subsequently determined to present high levels of security risk are subject to the more substantive requirements of the CFATS regulation.[20]

The CFATS regulation outlines a specific process for how ISCD is to administer the CFATS program. A chemical facility that possesses any of the 322 chemicals of interest in the quantities that meet or exceed a threshold quantity is required to use ISCD's Chemical Security Assessment Tool, a web-based application through which owners and operators of chemical facilities provide information about the facility to ISCD. If ISCD determines that a facility is high risk, the facility must complete and submit to ISCD a standard security plan, expedited security plan, or Alternative Security Program. Tier 1 and tier 2 facilities must use the standard security plan or Alternative Security Program, while tier 3 and tier 4 facilities also have the option to use the expedited security plan. For a facility that submits a standard security plan or Alternative Security Program, ISCD reviews it for compliance with CFATS. If compliant, ISCD issues a letter of authorization and conducts an authorization inspection.[21] If the facility passes the authorization inspection, ISCD issues a letter of approval and the facility implements the approved security plan or program.[22] Subsequently, ISCD conducts compliance inspections to

[19]Such facilities can include food-manufacturing facilities that use chemicals of interest in the manufacturing process, universities that use the chemicals to do experiments, or warehouses that store ammonium nitrate, among others. Under the CFATS Act of 2014, such a facility may be recognized as a "chemical facility of interest." See 6 U.S.C. § 621(2). Consistent with law and regulation, certain facilities—including, in general, facilities regulated under the Maritime Transportation Security Act of 2002 (Public Law 107-295, 116 Stat. 2064), public water systems or wastewater treatment facilities, facilities owned and operated by the Department of Defense or the Department of Energy, and facilities subject to regulation by the Nuclear Regulatory Commission or in accordance with the Atomic Energy Act of 1954—are not subject to regulation under CFATS and are referred to as excluded facilities. 6 USC § 621(4).

[20]See generally 6 C.F.R. pt. 27, subpt. B.

[21]An authorization inspection consists of an initial, physical review of the facility to determine if the Top-Screen, security vulnerability assessment, and site security plan accurately represent and address the risks for the facility. The Top-Screen is the initial screening tool whereby a chemical facility in possession of a chemical of interest at the requisite thresholds is to provide data to ISCD, including the name and location of the facility and the chemicals of interest and their quantities at the site.

[22]If ISCD determines that the site security plan or Alternative Security Program does not satisfy CFATS requirements, ISCD notifies the facility of any deficiencies and the facility must submit a revised security plan or Alternative Security Program to correct them.

confirm that the facility has implemented its approved security plan or program.

For tier 3 or tier 4 facilities that choose to submit the expedited security plan, ISCD reviews the expedited plan to determine if it is sufficient and, if so, issues a letter of acceptance. If the expedited plan is determined to be facially deficient, the facility is no longer eligible to participate in the EAP and must submit a standard security plan or Alternative Security Program.[23] For expedited facilities that receive a letter of acceptance, ISCD does not conduct an authorization inspection because the CFATS Act of 2014 does not provide for this inspection at expedited facilities. However, ISCD intends to subsequently conduct compliance inspections to confirm that the expedited facility has implemented its approved security plan.

Regarding the EAP, the CFATS Act of 2014 states that, among other things, DHS is to

- issue guidance for EAP facilities not later than 180 days after enactment of the act that identifies specific security measures sufficient to meet Risk-Based Performance Standards;
- approve a facility's expedited security plan if it is not facially deficient based upon a review of the expedited plan;
- verify a facility's compliance with its expedited security plan through a compliance inspection;[24]

[23]A facially deficient site security plan is defined as a security plan that does not support a certification that the security measures in the plan address the security vulnerability assessment and Risk-Based Performance Standards, based on a review of the facility's site security plan, the facility's Top-Screen, the facility's security vulnerability assessment, or any other information that the facility submits to ISCD or ISCD obtains from a public source or other source. 6 U.S.C. § 621(7). Specifically, ISCD determines that an expedited security plan is deficient if it: does not include existing or planned measures which satisfy applicable Risk-Based Performance Standards; materially deviates from at least one EAP security measure without adequately explaining that the facility has a comparable security measure; and/or contains a misrepresentation, omission, or inaccurate description of at least one EAP security measure. A facility is to implement any planned security measures within 12 months of the expedited security plan's approval because ISCD has determined that it is unlikely that all required security measures will be in place when a facility submits its expedited plan to ISCD.

[24]ISCD officials stated that, although the CFATS Act of 2014 provides that DHS "may" conduct compliance inspections at EAP facilities, ISCD intends to conduct compliance inspections at all EAP facilities.

- require the facility to implement additional security measures or suspend the facility's certification if, during or after a compliance inspection, security measures are insufficient to meet Risk-Based Performance Standards based on misrepresentation, omission, or an inadequate description of the site;[25] and
- conduct a full evaluation of the EAP and submit a report on the EAP not later than 18 months after the date of enactment of the act to Congress.

DHS Has Fully Implemented the EAP and Reported to Congress on Its Assessment of the Program

DHS Has Issued Guidance for the EAP and Fully Implemented the Program

On May 12, 2015, DHS issued EAP guidance for eligible facilities to use to prepare their expedited plans. DHS fully implemented the EAP about a month later when facilities could submit expedited security plans and certification forms to ISCD. Consistent with the act, DHS developed the guidance within 180 days after the date the act was enacted and identified specific security measures that are sufficient to meet Risk-Based Performance Standards applicable to facilities under DHS's standard security plan process.[26] The guidance is intended to help facilities prepare and submit their expedited security plans and certifications to ISCD, and includes an example that identifies specific (i.e., prescriptive) security measures that facilities are to have in place. Appendix I provides an example of the EAP's prescriptive security measures and shows the measures that an EAP facility is to have in place to respond to a threat or actual theft or release of a chemical of interest.

[25]Certification is defined as a document signed under penalty of perjury by the owner or operator of an expedited approval facility and submitted with an expedited site security plan that certifies compliance with all of the requirements contained in 6 U.S.C. § 622(c)(4)(C).

[26]See 6 U.S.C § 622(c)(4)(B)(i). The act was enacted on December 18, 2014.

ISCD officials told us that, in developing prescriptive security measures for the EAP, they considered various sources, including:

- lessons learned from approving prior standard security plans and Alternative Security Programs for tier 3 and tier 4 facilities and conducting inspections at these facilities; [27]
- Risk-Based Performance Standards used to develop a standard security plan or Alternative Security Program; and
- relevant academic literature, and security directives, guidelines, standards, and regulations issued by other federal agencies, such as the U.S. Army and the Department of Labor.

ISCD officials told us that they developed the EAP security measures with clear, specific guidance, so that facility officials would have the information needed to successfully obtain approval of their expedited security plan upon submission. The CFATS Act of 2014 allows facilities to submit only one expedited plan to DHS. Specifically, if ISCD determines that an expedited plan is facially deficient due to an error, the act does not allow facility officials to correct the error and resubmit the plan. In addition, ISCD officials said that prescriptive, clear, and easily understood EAP security measures are needed because the act requires DHS to approve an expedited plan that has all applicable prescribed security measures and does not provide for an authorization inspection under the EAP. Therefore, ISCD's goal in developing required security measures for an expedited security plan was to ensure that a facility had adequate security in place until inspectors could conduct a compliance inspection at the facility approximately 1 year after approving the plan.

ISCD officials also stated that, before and after implementing the EAP, they reached out to industry representatives to ensure that eligible facilities were aware of the EAP and its availability as an option to the standard security plan and Alternative Security Program. Specifically, ISCD held meetings with officials representing the Chemical Sector Coordinating Council, the Food and Agriculture Sector Coordinating Council, and the Oil and Natural Gas Subsector Coordinating Council before issuing the EAP guidance and also contacted them after doing so.

[27]ISCD officials analyzed lessons learned from approving standard security plans and Alternative Security Programs to identify which security measures for the standard plans were critical to approving a facility's plan. The officials used that knowledge and experience to help them decide which security measures to require in the expedited security plan.

ISCD also made presentations about the EAP at the Chemical Sector Security Summit in July 2015, and to other groups, including three labor unions prior to implementing the EAP.[28] In addition, ISCD chemical security inspectors and other staff routinely discuss the EAP when conducting CFATS-related outreach.

Officials we interviewed at the three coordinating councils confirmed that DHS had contacted them about the EAP. Also, officials from 8 of the 11 industry organizations we interviewed said they have been generally pleased with DHS's efforts to communicate with them about the CFATS program in recent years. However, officials from a Sector Coordinating Council stated that ISCD did not accept the council's offers to assist in developing the EAP guidance and were concerned that ISCD may not accept future offers to work on CFATS issues. A senior ISCD official stated that ISCD did not accept the council's offers to assist in developing the EAP guidance because the CFATS Act of 2014 required DHS to develop the guidance within 6 months of enactment, which did not allow time to involve all interested stakeholders in developing it. The ISCD official stated that ISCD continues to value stakeholder input, appreciates the desire of Sector Coordinating Council members and other stakeholders to provide input on CFATS materials, and plans to seek input from Sector Coordinating Councils and other stakeholders, as appropriate, on future relevant issues.

ISCD officials also told us that they developed draft, standard operating procedures to evaluate expedited security plans and conduct compliance inspections, and that officials used the draft procedures to evaluate expedited plans since the EAP's implementation. ISCD staff who review expedited security plans have received training on how to do this and vetting an expedited plan is relatively simple and straightforward because it does not require extensive analysis, according to ISCD officials. Specifically, ISCD staff review an expedited security plan to determine if facility officials have checked all required boxes for applicable security measures, adequately explained any planned security measures or

[28]The Chemical Sector Security Summit is an industry-wide networking and educational event cosponsored by DHS and the Chemical Sector Coordinating Council to provide a forum for representatives from the chemical community to exchange information, network with other security professionals, share best practices, learn about chemical security regulations, and gain insight into the roles of state, local, and federal agencies and departments involved in chemical security.

material deviations, and signed the required certification.[29] If ISCD staff concludes that all of these things have been done, they recommend that the ISCD Director approve the expedited security plan. ISCD staff prepares a summary of the review, including the recommendation, and provides it to the Director. These standard operating procedures were approved on May 25, 2017.

DHS's Report on the EAP Discussed All Statutory Elements

DHS's report to Congress on the EAP, issued on August 2, 2016, discussed all elements listed in the CFATS Act of 2014, but did not quantify costs associated with the EAP because most of DHS's initial costs were for salary and benefits and DHS did not require its employees to track the hours they worked on the EAP.[30] DHS also did not quantify associated costs to the regulated community, but stated that it expects that these costs were very low. In addition, DHS's report did not include a recommended frequency of compliance inspections at facilities that use the program because, currently, there is no mandated frequency for any facility regardless of the type of security plan submitted. DHS noted that it would prioritize conducting an initial compliance inspection at an expedited facility over inspection of a similar facility that received approval of a traditional (i.e., standard) security plan or Alternative Security Program, in part, because that would be the first inspection conducted at the expedited facility. In addition, the report stated that, among other things, it was difficult to assess the effect of the EAP on DHS operations and the operations of facilities because only a single facility had participated in the EAP at the time the report was issued. Our analysis of the DHS report and follow-up discussions with ISCD officials is discussed below.

- **Assess the number of eligible facilities that used the EAP versus the standard process to develop and submit a site security plan.** DHS reported that, as of June 2, 2016, it assigned a final tier of 3 or 4 to 2,244 facilities (806 tier 3 facilities and 1,438 tier 4 facilities). Of

[29]An expedited security plan must comply with the EAP guidance; however, the expedited plan may propose an alternative security measure that meets the relevant Risk-Based Performance Standards. If a facility chooses a security measure that materially deviates from a measure specified in the guidance, the expedited plan must identify the deviation for the specific security measure and explain how the new measure meets relevant Risk-Based Performance Standards. See 6 U.S.C. § 622(c)(4)(B)(ii).

[30]Under the CFATS Act of 2014, the DHS report was required to be submitted by June 2016. ISCD officials did not provide an explanation for why the report was late, other than that DHS missed the deadline.

these facilities, only one facility (a tier 4 facility) submitted an expedited security plan, while 2,194 facilities had submitted a security plan or Alternative Security Program using the standard process, and 49 facilities had yet to submit a security plan or Alternative Security Program.[31]

- **Assess the EAP's impact on the backlog for site security plan approvals and authorization inspections.**[32] DHS reported that, with only a single facility electing to submit an expedited security plan, the EAP had no noticeable impact on DHS's projected completion date for all authorization inspections and site security plan approvals. ISCD officials told us that if enough facilities use the EAP in the future, DHS would evaluate the EAP's effect on its CFATS operations.
- **Assess the ability of EAP facilities to submit sufficient site security plans.** DHS reported that the only facility to submit an expedited security plan was able to submit a sufficient plan.
- **Assess any impact of the EAP on the security of chemical facilities.** DHS reported that it is difficult to assess the impact of the EAP on the security of chemical facilities because only one facility submitted an expedited security plan. DHS noted that the public availability of the EAP guidance would likely have a positive impact on chemical facility security because the guidance can serve as reference material for any facility looking to develop a security plan, regardless of whether that facility is regulated under CFATS. ISCD officials told us that if enough facilities use the EAP in the future, DHS would evaluate the EAP's effect on the security of chemical facilities.
- **Identify any costs and efficiencies associated with the EAP.** DHS reported that it expended significant internal resources to comply with the statutory requirement to develop an EAP, but DHS did not quantify the cost associated with the EAP. According to DHS, the resources expended included costs to develop EAP processes and procedures, and develop the associated guidance and outreach materials. ISCD officials told us that most of DHS's initial costs were for salary and benefits for federal employees working on the EAP, including policy,

[31]Later in this report, we discuss factors for low participation in the EAP.

[32]In 2015, we estimated that it could take between 9 and 12 months for ISCD to review and approve security plans for approximately 900 remaining facilities (GAO-15-614). In 2016, DHS reported that it had eliminated the backlog of approvals for site security plans and Alternative Security Programs. DHS, *Implementation Status of the Chemical Facility Anti-Terrorism Standards*, Second Semiannual, Fiscal Year 2016, Dec. 9, 2016, Fiscal Year 2016 Report to Congress.

compliance, and legal staff who developed the EAP guidance, and information technology staff who updated the Chemical Security Assessment Tool. However, ISCD officials also told us that they were unable to quantify these costs because headquarters employees are only required to track overall hours worked each day versus time spent on individual tasks. ISCD officials stated that they have expended, and expect to continue to expend, minor funding amounts to keep the EAP operational. DHS also reported that it was unable to discern how much time and resources members of the regulated community or other stakeholders expended on activities, such as reviewing EAP proposals or considering whether to use the EAP. However, DHS stated that it expects that EAP costs to the regulated community were very low.

- **Recommend the frequency of compliance inspections that may be required for EAP facilities.** DHS discussed factors that can influence the frequency of compliance inspections, but did not quantify a recommended frequency for facilities in the EAP because, currently, there is no mandated frequency for any facility regardless of the type of security plan submitted. According to DHS, a variety of factors can influence the frequency of compliance inspections regardless of the type of site security plan the facility submits, including the facility's risk-based tier and previous compliance history, the corporate owner's compliance history, and the number and type of planned measures in the facility's approved security plan. The report also stated that DHS would consider if a facility elected to submit an expedited security plan when determining the timing of the facility's initial compliance inspection and frequency of subsequent inspections. Although DHS did not quantify a recommended frequency of compliance inspections, it noted that the election to use an expedited security plan would have the most impact on scheduling the initial compliance inspection because that would be the first inspection DHS would conduct at the facility. In addition, DHS would prioritize conducting an initial compliance inspection at an expedited facility over inspection of a similar facility that received approval of a traditional (i.e., standard) security plan or Alternative Security Program.

Low EAP Participation May Be Due to Various Factors

Two Chemical Facilities Have Used the EAP since Its Inception

According to DHS, as of April 2017, 2 of the 2,496 eligible facilities had used the EAP since ISCD implemented it; however, one of the two facilities was no longer in the EAP because ISCD no longer considers the facility to be high risk. ISCD had approved both facilities' expedited security plans—one before DHS issued the aforementioned report to Congress and one after the report. ISCD officials stated that they have not assessed why only two facilities have used the EAP and do not intend to do so because they did not have a preconceived number of facilities that they expected to use it. They also said that the EAP is one of three options—the expedited security plan, the standard security plan, and the Alternative Security Program—that tier 3 and tier 4 facilities can use. ISCD does not encourage facilities to use the EAP or discourage facilities from using it because facility officials are in the best position to decide which approach is the best option for their facility.

Officials representing the two EAP chemical facilities told us that their companies involve small operations that store a single chemical of interest on site and do not have staff with extensive experience or expertise in chemical security. Officials from both facilities said they used the EAP instead of a standard site security plan or Alternative Security Program because the EAP would reduce the time and cost to prepare and submit their security plans. Officials from both facilities also stated that the EAP's prescriptive nature helped them to quickly determine the security measures required to be in their site security plans. For example, the contractor who prepared the site security plan for one of the two EAP facilities said that the facility probably saved $2,500 to $3,500 in consulting fees by using the EAP instead of a standard security plan. According to ISCD, the first compliance inspection at the one remaining EAP facility is scheduled to start later in calendar year 2017.

ISCD and Stakeholders Identified Several Factors That May Explain Why the EAP Has Not Been More Widely Used

ISCD and industry stakeholders we interviewed identified several factors that may explain why the EAP has not been more widely used, as discussed below.

Timing of the EAP's Implementation. ISCD officials stated that the timing of the EAP's implementation may be the primary reason that only two facilities have used it. The officials explained that, by the time ISCD had implemented the EAP, the majority of eligible facilities had already submitted standard site security plans or Alternative Security Programs to ISCD, so it was not worthwhile for the facilities to start over again to use the EAP. For example, ISCD officials told us that they had already approved standard security plans and Alternative Security Programs from about 61 percent (1,463 of approximately 2,400) of facilities that had been assigned to tier 3 or tier 4 prior to the EAP's implementation.[33] Also, officials from 5 of the 11 industry organizations we interviewed stated that the timing of the EAP's implementation resulted in limited interest in using the EAP.[34]

Prescriptive Nature of the EAP. As previously discussed, the CFATS Act of 2014 required DHS to develop specific security measures for the EAP that are sufficient to meet Risk-Based Performance Standards. ISCD officials and officials from 6 of the 11 industry organizations we interviewed stated that the prescriptive security measures required in the expedited security plan likely deterred some facilities from using the EAP. According to ISCD officials, some industry officials think that certain EAP-required security measures are too strict for tier 3 and tier 4 facilities. Officials we interviewed from 5 of the 11 industry organizations said that some, if not most, EAP-required security measures are more robust or strict than they should be for tier 3 and tier 4 facilities; however, officials from a Sector Coordinating Council and a member organization said that the EAP's required security measures are fair or appropriate for tier 3 and

[33]An ISCD official stated that the number of tier 3 and tier 4 facilities has fluctuated over the last 10 years. For example, according to ISCD, from 2007 through 2015, more than 3,000 previously-tiered facilities have eliminated, reduced, or modified their chemical holdings and/or processes and are no longer considered high risk. As a result of this and other factors (e.g., facilities closing, tier 3 and tier 4 facilities making changes resulting in an increase in tier to tier 1 or tier 2), the number of EAP-eligible facilities changed from 2,496 to about 2,400 over time.

[34]Officials we interviewed from 6 of the 11 industry organizations did not make a comment about whether the timing of the EAP's implementation resulted in limited interest in using the EAP.

tier 4 facilities.[35] ISCD officials agreed that some EAP required security measures are strict because the CFATS Act of 2014 requires that DHS develop specific security measures and approve expedited security plans that are determined to not be facially deficient based only on a review of the plan. For example, an industry official told us that a security measure pertaining to screening and inspection of vehicles is too strict. Specifically, the EAP guidance states that a facility must screen and inspect all vehicles for firearms, explosives, or certain materials prior to allowing vehicles access to the facility's perimeter by visually inspecting the vehicle, using a trained explosive detection dog team, under/over vehicle inspection systems, or cargo inspection systems. ISCD officials told us that this security measure is required because ISCD would not be able to evaluate the capability of a facility's random or percentage-based screening and inspection program by doing a review of the facility's expedited security plan; therefore, ISCD requires that EAP facilities apply this requirement to all vehicles prior to accessing a facility's perimeter.

However, ISCD officials and officials from 4 of 11 industry organizations also stated that the EAP's prescriptive measures actually could encourage some facilities to use the EAP.[36] For example, officials from an industry organization stated that smaller facilities often lack staff with the expertise needed to prepare a standard site security plan or Alternative Security Program and may prefer the EAP because it clearly states what a facility is required to do to meet security measures. This was consistent with the views of the officials representing the two facilities that submitted EAPs, as discussed earlier.

Lack of an Authorization Inspection under the EAP. As previously discussed, ISCD conducts an authorization inspection at facilities using the standard process, but does not conduct this inspection at facilities using the EAP. ISCD officials stated that the lack of an authorization inspection under the EAP may discourage some facilities from using it because some facility officials have told ISCD that this inspection

[35]Officials from 4 of the 11 industry organizations we interviewed did not make a comment about whether the EAP's required security measures are more robust or strict, or fair or appropriate for tier 3 and tier 4 facilities.

[36]Some industry officials stated that the EAP's prescriptive security measures could deter some facilities from using the EAP, but encourage other facilities to use the EAP. Also, officials from 3 of the 11 industry organizations we interviewed did not make a comment about whether the EAP's prescriptive measures deterred some facilities from using the EAP or encouraged some facilities to use the EAP.

provides useful information about their facility's security. However, ISCD officials also said that some facilities may prefer the lack of an authorization inspection under the EAP because this expedites the approval process for a site security plan compared to the process for a standard security plan or Alternative Security Program.

Certification Form Required for the EAP. An ISCD official and an industry official we interviewed told us that the certification form that a facility official must sign under penalty of perjury and submit to ISCD with the expedited security plan, may deter some facilities from using the EAP. For example, the DHS official stated that the form contains strict requirements and could result in the signing official being legally liable and subject to penalties in certain circumstances. However, officials for the two facilities that submitted expedited security plans and certification forms to ISCD told us that they were not concerned about signing the form.

The Effect of Recent Changes to the CFATS Program on Future Use of the EAP Is Uncertain

Two other factors that could influence facilities' participation in the EAP are the introduction of revised processes for (1) facilities to provide information to ISCD and (2) ISCD to determine the risk tier for each facility. ISCD officials stated that, in fall 2016, they implemented a revised Chemical Security Assessment Tool for facilities to provide information to ISCD in response to industry concerns, such as asking facilities to answer duplicate questions. In the same time frame, ISCD implemented a revised risk-tiering methodology in response to our prior reports and stakeholder concerns about not addressing all elements of risk (threat, vulnerability, and consequence). ISCD officials said they revised the risk-tiering methodology to enhance its ability to consider the elements of risk associated with a terrorist attack.[37]

The revised Chemical Security Assessment Tool, called the Chemical Security Assessment Tool 2.0, includes a revised Top-Screen and a streamlined version of the standard site security plan.[38] ISCD officials said that a primary reason they revised the assessment tool was to

[37]ISCD has provided documentation to us with the details of the revised risk-tiering methodology; we intend to evaluate it in the coming months.

[38]The Top-Screen is the initial screening tool whereby a chemical facility in possession of a chemical of interest at the requisite thresholds is to provide data to ISCD, including the name and location of the facility and the chemical(s) of interest and their quantities at the site.

eliminate duplication and confusion associated with the original standard security plan. The streamlined security plan, in ISCD officials' view, flows more logically, is more user-friendly, requires facility officials to write less narrative, does not have ambiguous questions, and pre-populates data from one part to another, so users do not have to re-type the same information multiple times. According to ISCD officials, industry feedback about Chemical Security Assessment Tool 2.0 has been very positive. Officials in 9 of the 11 industry organizations we interviewed told us that they have positive views about the revised assessment tool and that it is better than the original assessment tool. For example, officials from 5 of the 11 industry organizations stated that ISCD had improved the assessment tool by streamlining or eliminating duplicative questions. If the updated tool proves easier to use, it could affect future interest in using the expedited program.

Regarding the revised tiering methodology, ISCD initiated a phased approach to re-tier about 27,000 facilities. ISCD officials said these facilities must re-submit Top-Screens using Chemical Security Assessment Tool 2.0 and the revised tiering methodology will be used to determine if each facility is high risk and, if so, assign the appropriate risk tier to the facility. According to a senior ISCD official, the re-tiering efforts are resulting in shifts in the risk assessments for some facilities due to the revised tiering methodology and because many facilities have not submitted new information in 7 or 8 years; however, dramatic shifts in the risk tiers of a large number of facilities are not expected. Nevertheless, ISCD is uncertain about the effect that Chemical Security Assessment Tool 2.0 and the revised tiering methodology will have on the future use of the EAP because ISCD cannot predict the extent to which facilities may be

- re-assigned from tier 1 or tier 2 to tier 3 or tier 4, or vice versa;
- assigned to tier 3 or tier 4 and submit an expedited security plan instead of a streamlined standard plan or Alternative Security Program, or vice versa;
- new to CFATS and assigned to tier 3 or tier 4; or
- no longer considered to be high risk.[39]

[39]As previously discussed, one of the two EAP facilities that has submitted data via Chemical Security Assessment Tool 2.0 is no longer a high-risk facility after applying the revised tiering methodology. Thus, the facility no longer needs to comply with its expedited security plan.

Given that only one facility is currently covered by the EAP, and about 27,000 facilities are to ultimately re-submit Top-Screens using Chemical Security Assessment Tool 2.0 and be tiered using the revised tiering methodology, it is too early to tell what impact, if any, the revised CFATS process will have on the future use of the EAP.

Agency Comments

We provided a draft of this report to DHS for review and comment. DHS did not provide formal comments, but did provide a technical comment, which we incorporated, as appropriate.

We are sending copies of this report to interested congressional committees and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (404) 679-1875 or CurrieC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Chris P. Currie
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

The Honorable Greg Walden
Chairman
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

Appendix I: Example of a Section in an Expedited Approval Program Site Security Plan

The following security measures are from Section D of the site security plan example for the Expedited Approval Program.[1] For facilities that prepare an expedited security plan and submit it to the Department of Homeland Security (DHS), facility officials are to put a checkmark next to each applicable security measure that the facility has in place. For each applicable security measure that the facility does not have in place, facility officials are to explain the security measure planned to be implemented in the next 12 months. If the facility has a material deviation from a security measure, facility officials are to explain compensatory measures that provide comparable security.

Section D: Response Measures (Risk-Based Performance Standards 9, 11, 13, and 14)

D.1 Response Planning

D.1.1 ___ The facility has a defined emergency and security response organization in order to respond to site emergencies and security incidents.

D.1.2 ___ The facility has a crisis management plan which includes emergency response procedures, security response plans, and post-incident security plans (post-terrorist attack, security incident, natural disaster, etc.).

For Release facilities only:

D.1.2.1 ___ The facility has additional portions to their crisis management plan, which include emergency shutdown plans, evacuation plans, re-entry/recovery plans, and community notification plans to account for response to Release chemicals of interest.

___ The facility is not regulated for Release chemicals of interest.

D.1.3 ___ The facility has designated individual(s) responsible for executing each portion of the crisis management plan and individual(s) have been trained to execute all duties.

D.1.4 ___ The facility has the appropriate resources (staff, emergency/response equipment, building space, communications

[1]DHS, *DHS Guidance for the Expedited Approval Program* (Washington, D.C.: May 12, 2015).

equipment, process controls/safeguards, etc.) to execute all response plans. Emergency equipment includes at least one of the following:

- A radio system that is redundant and interoperable with law enforcement and emergency response agencies.
- At least one backup communications system, such as cell phones/desk phones.
- An emergency notification system (e.g., a siren or other facility-wide alarm system).
- Automated control systems or other process safeguards for all process units to rapidly place critical asset(s) in a safe and stable condition and procedures for their use in an emergency.
- Emergency safe-shutdown procedures for all process units.

D.1.5 ___ All facility personnel have been trained on all response plans and response plans are exercised on a regular basis and at a minimum of biennially.

D.1.6 ___ The facility has an active outreach program with local first responders (Police Department and Fire Department) which includes providing response documentation to agencies, providing facility layout information to agencies, inviting agencies to facility orientation tours, notifying agencies of the facility's chemicals of interest (regulated chemicals of interest and other chemical holdings identified on Appendix A) and security concern, and maintaining regular communication with agencies.

D.2 Elevated and Specific Threats (Risk-Based Performance Standards 13 and 14):

D.2.1 ___ The facility has a documented process for increasing security measures commensurate to the designated threat level during periods of elevated threats tied to the National Terrorism Advisory System and when notified by DHS of a specific threat.

D.2.2 ___ The facility will begin to execute security measures for elevated and specific threats within 8 hours of notification.

D.2.3 ___ The facility will execute the following measures as a result of an elevated or specific threat:

- Coordinate with Federal, state, and local law enforcement agencies.
- Increase detection efforts through either dedicated monitoring of security systems (Intrusion Detection System (IDS) or Closed Circuit

Television (CCTV)), increased patrols of the perimeter and/or asset area(s), or stationing of personnel at access points and/or asset area(s).

- For Theft/Diversion and Sabotage facilities only, increase frequency of outbound screening and inspections.
- For Sabotage facilities only, increase monitoring of outbound shipments.
- For Release facilities only, increase frequency of inbound screening and inspections.

Response Planned Measures

___ The facility does not have existing security measures for one or more of the required items above, but will implement the security measure through a planned measure no later than 12 months of approval as described below:

Material Deviation

___ The facility has materially deviated from the above response measures; however, the facility has incorporated compensatory measures, which offer comparative security to the requirements in Section D - Response and meet the security concerns in the relevant portions of the Risk-Based Performance Standards as follows:

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Chris P. Currie, at (404) 679-1875 or CurrieC@gao.gov

Staff Acknowledgments

In addition to the contact named above, John Mortin, Assistant Director, and Joseph E. Dewechter, Analyst-in-Charge, managed this audit engagement. Chuck Bausell, Michele Fejfar, Tracey King, Michael Lenington, and Claire Peachey made significant contributions to this report.