United States Government Accountability Office

Report to Congressional Requesters

January 2021

CHEMICAL SECURITY

Overlapping Programs Could Better Collaborate to Share Information and Identify Potential Security Gaps

GAO-21-12

GAO@100 Highlights

Highlights of GAO-21-12, a report to congressional requesters

January 2021

CHEMICAL SECURITY

Overlapping Programs Could Better Collaborate to Share Information and Identify Potential Security Gaps

Why GAO Did This Study

Facilities with hazardous chemicals could be targeted by terrorists to inflict mass casualties or damage. Federal regulations applicable to chemical safety and security have evolved over time as authorizing statutes and regulations established programs for different purposes, such as safety versus security, and with different enforcement authorities. GAO has reported that such programs may be able to achieve greater efficiency where overlap exists by reducing duplication and better managing fragmentation.

GAO was asked to review issues related to the effects that overlap, duplication, and fragmentation among the multiple federal programs may have on the security of the chemical sector. This report addresses the extent to which (1) such issues may exist between CFATS and other federal programs, and (2) the CFATS program collaborates with other federal programs. GAO analyzed the most recent available data on facilities subject to nine programs from DHS, EPA, ATF, and DOT; reviewed and analyzed statutes, regulations, and program guidance; and interviewed agency officials.

What GAO Recommends

GAO is making seven recommendations, including that DHS, EPA, ATF, and DOT identify facilities subject to multiple programs; DHS clarify guidance; and DHS and EPA assess security gaps. Agencies generally agreed with six; EPA did not agree with the recommendation on gaps. GAO continues to believe it is valid, as discussed in the report.

View GAO-21-12. For more information, contact Nathan Anderson, 206-287-4804, AndersonN@gao.gov

What GAO Found

Eight federal programs addressing chemical safety or security from four departments or agencies that GAO reviewed contain requirements or guidance that generally align with at least half of the Department of Homeland Security's (DHS) 18 Chemical Facility Anti-Terrorism Standards (CFATS) program standards. At least 550 of 3,300 (16 percent) facilities subject to the CFATS program are also subject to other federal programs. Analyses of CFATS and these eight programs indicate that some overlap, duplication, and fragmentation exists, depending on the program or programs to which a facility is subject. For example,

- six federal programs' requirements or guidance indicate some duplication with CFATS. CFATS program officials acknowledge similarities among these programs' requirements or guidance, some of which are duplicative, and said that the CFATS program allows facilities to meet CFATS program standards by providing information they prepared for other programs.
- more than 1,600 public water systems or wastewater treatment facilities are excluded under the CFATS statute, leading to fragmentation. While such facilities are subject to other programs, those programs collectively do not contain requirements or guidance that align with four CFATS standards. According to DHS, public water systems and wastewater treatment facilities are frequently subject to safety regulations that may have some security value, but in most cases, these facilities are not required to implement security measures commensurate to their level of security risk, which may lead to potential security gaps.

The departments and agencies responsible for all nine of these chemical safety and security programs—four of which are managed by DHS, three by the Environmental Protection Agency (EPA), and one each managed by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Department of Transportation (DOT)—have previously worked together to enhance information collection and sharing in response to Executive Order 13650, issued in 2013. This Executive Order directed these programs to take actions related to improving federal agency coordination and information sharing.

However, these programs have not identified which facilities are subject to multiple programs, such that facilities may be unnecessarily developing duplicative information to comply with multiple programs. Although CFATS allows facilities to use information they prepared for other programs, CFATS program guidance does not specify what information facilities can reuse. Finally, DHS and EPA leaders acknowledged that there are differences between CFATS requirements and the security requirements for public water systems and wastewater treatment facilities, but they have not assessed the extent to which potential security gaps may exist. By leveraging collaboration established through the existing Executive Order working group, the CFATS program and chemical safety and security partners would be better positioned to minimize unnecessary duplication between CFATS and other programs and better ensure the security of facilities currently subject to fragmented requirements.

Contents

Figures

Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AWIA	America's Water Infrastructure Act of 2018
CISA	Cybersecurity and Infrastructure Security Agency
CFATS	Chemical Facility Anti-Terrorism Standards
DOT	Department of Transportation
DHS	Department of Homeland Security
EPA	U.S. Environmental Protection Agency
Hazmat	hazardous material
MTSA	Maritime Transportation Security Act of 2002
RCRA	Resource Conservation and Recovery Act
RMP	Risk Management Program
TSA	Transportation Security Administration
TSDF	Treatment, Disposal, and Storage Facilities
Coast Guard	U.S. Coast Guard
Water Infrastructure Act working group	America's Water Infrastructure Act Executive Order 13650 Chemical Facility Safety and Security Working Group

441 G St. N.W.
Washington, DC 20548

January 21, 2021

Congressional Requesters

The United States has thousands of facilities that produce, use, or store hazardous chemicals that, if not properly safeguarded, could be used by terrorists to inflict mass casualties and damage. These chemicals, if released from a facility, stolen, or diverted and used to create explosive devices, chemical weapons, or other weapons, could cause significant harm to surrounding populations. Past incidents in the United States and overseas demonstrate the danger these chemicals pose. For example, in April 2018, attacks using chlorine in Syria resulted in dozens of deaths and hundreds of injuries. In November 2019, an accidental explosion at a waterfront Texas chemical plant that manufactures butadiene resulted in mandatory evacuations for thousands of residents within a four-mile radius.[1] In August 2020, Hurricane Laura caused a chlorine leak at a chemical facility in Lake Charles, Louisiana, leading to shelter in place orders for the local population because of the dangerous cloud created by the related chemical fire.

In 2007, the Department of Homeland Security (DHS) established its Chemical Facility Anti-Terrorism Standards (CFATS) program to assess the risks posed by U.S. chemical facilities and classify those designated as high-risk, among other things.[2] DHS's Cybersecurity and Infrastructure Security Agency (CISA) manages the program. DHS established in

[1]The major use of butadiene is in the production of tires, according to the American Chemistry Council. Butadiene is also consumed in the manufacture of polymers, latexes, and plastics.

[2]Section 550 of the Department of Homeland Security Appropriations Act, 2007, required vulnerability assessments and the development and implementation of site security plans for such facilities. Pub. L. No. 109-295, § 550, 120 Stat. at 1388-89. DHS published the CFATS interim final rule in April 2007. 72 Fed. Reg. 17,688 (Apr. 9, 2007) (codified as amended at 6 C.F.R. pt. 27). Appendix A to the rule, published in November 2007, lists 322 chemicals of interest and the screening threshold quantities for each. 72 Fed. Reg. 65,396 (Nov. 20, 2007) (codified at 6 C.F.R. pt. 27, App. A). 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. 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.

regulation the chemicals it considers to be potentially dangerous and posing a security risk—known as chemicals of interest.[3] The CFATS program generally requires any facility in possession of a chemical of interest above a certain threshold quantity to report its chemical holdings and other data to DHS. After receiving this information, DHS determines a facility's risk level. High-risk facilities must address comprehensive security measures across the CFATS program's 18 risk-based performance standards (CFATS standards).[4]

Some of these high-risk facilities are subject to oversight by other federal departments and agencies, including the Transportation Security Administration (TSA) and U.S. Coast Guard (Coast Guard) within DHS; the Environmental Protection Agency (EPA); the Department of Transportation (DOT); the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and the Department of Labor. However, not all facilities that possess a chemical of interest above the threshold quantity are subject to the CFATS program and its security standards. Certain types of facilities are excluded by law under the CFATS program, and some of those facilities are subject to other regulatory programs that address chemical security.[5]

In August 2013, Executive Order 13650 recognized the need for coordination amongst these numerous chemical safety and security programs aimed at reducing the risks associated with hazardous chemicals. It established a Chemical Facility Safety and Security Working Group (working group)—led by DHS, EPA, and the Department of Labor, along with representation from ATF and DOT, among others. Among other things, the executive order acknowledged that there are numerous federal chemical safety and security programs and, recognizing the overlap between some of these programs, directed the working group to take certain actions to enhance information collection and sharing across

[3]6 C.F.R. pt. 27, app. A.

[4]The 18 risk-based performance standards identify areas for which a facility's security posture are to be examined, such as perimeter security, access control, and cyber security. 6 C.F.R. § 27.230

[5]Under the CFATS program, excluded facilities include all facilities defined as a public water system or wastewater treatment works, which are regulated by the EPA, facilities owned or operated by the Department of Defense or Department of Energy, regulated by the Nuclear Regulatory Commission, or facilities regulated under the Maritime Transportation Security Act of 2002 by the Coast Guard. 6 U.S.C. § 621(4).

agencies to support more informed decision-making, streamline reporting requirements, and reduce duplicative efforts, among other things.[6]

You asked us to review possible overlap, duplication, and fragmentation amongst the multiple federal programs that regulate safety and security of the chemical sector. We have previously reported that agencies may be able to achieve greater efficiency and effectiveness by reducing or better managing overlap, duplication, and fragmentation.[7] This report evaluates (1) the extent to which overlap, duplication, and fragmentation may exist between CFATS and other federal programs that regulate chemical safety and security and (2) the extent to which the CFATS program collaborates with other federal programs to manage or avoid unnecessary duplication and fragmentation.

To evaluate the extent to which overlap, duplication, and fragmentation may exist between CFATS and other federal programs that regulate chemical safety and security we reviewed an executive order related to chemical safety and security, statutes, regulations, and other documents. Specifically, we focused on: (1) DHS' CFATS program, (2) the Coast Guard's Maritime Transportation Security Act of 2002 (MTSA) program, (3) TSA's rail security program, (4) TSA's pipeline security program, (5) ATF's explosive materials program, (6) EPA's America's Water Infrastructure Act (Water Infrastructure Act) program, (7) EPA's Risk

[6]On August 1, 2013, the President issued Executive Order 13650–*Improving Chemical Facility Safety and Security*, which called for federal action to improve chemical facility safety and security in coordination with owners and operators. Exec. Order No. 13,650, 78 Fed. Reg. 48,029 (Aug. 1, 2013). The executive order established a Chemical Facility Safety and Security working group, composed of representatives from DHS; EPA; and the Departments of Justice, Agriculture, Labor, and Transportation, and directed the working group to take actions to improve coordination with state and local partners; enhance federal agency coordination and information sharing; identify opportunities to modernize policies, regulations and standards; and work with stakeholders to identify and share best practices.

[7]See GAO's Duplication and Cost Savings web page for links to the 2011 to 2019 annual reports: http://www.gao.gov/duplication/overview. Using the framework established in our prior work on addressing fragmentation, overlap, and duplication, we use the following definitions for the purpose of assessing nine chemical programs that address safety and security: Overlap occurs when multiple programs have similar goals, engage in similar activities or strategies to achieve those goals, or target similar beneficiaries. Duplication occurs when two or more agencies or programs are engaging in the same activities or providing the same services to the same beneficiaries. Fragmentation occurs when more than one agency (or more than one organization within an agency) is involved in the same broad area of national interest and opportunities exist to improve customer service.

Management Program, (8) EPA's Resource Conservation and Recovery Act (RCRA) program, and (9) DOT's hazardous materials program.[8]

First, we compared programs' requirements and guidance to the CFATS program's 18 risk-based performance standards and associated guidance. We determined that a program's requirements generally align with a CFATS standard when the relevant statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take to meet the CFATS standard, to include in limited circumstances.[9] We considered program requirements and guidance to generally align with a CFATS standard when actions required or authorized under the program have a different purpose or goal but may have the same effect as actions taken pursuant to the CFATS standard. Second, we supplemented our analyses with written responses from each program, including asking each program whether it contained requirements or guidance for security measures beyond, in addition to, or more comprehensive than the CFATS standards. Third, we evaluated the extent to which alignment with CFATS indicates overlap, duplication, and fragmentation and applied our framework for identifying such conditions.[10] Finally, we analyzed comments to the CFATS proposed rule and DHS responses to identify the history of the program, including whether the

[8]We did not review all programs that address chemical safety and security, such as Department of Labor Occupational Safety and Hazards Administration requirements because they generally apply to labor issues beyond the scope of our review. The DOT also regulates the safety and security of liquefied natural gas transportation and storage under 49 C.F.R. part 193. Because the program focused on only one chemical common to the CFATS program—methane, we did not include this program in the scope of our review. We did not review Department of Energy or Department of Defense programs that apply to excluded facilities, which were beyond the scope of our review.

[9]Specifically, three analysts independently reviewed the programs' regulations, guidance, and other materials to determine if the programs contained requirements or guidance that generally aligned with each of the 18 CFATS standards. The three analysts compared their results and resolved any differences, and a senior attorney reviewed the unified assessment and supporting regulations, guidance, and other materials. For America's Water Infrastructure Act, we reviewed the statute, as there are no corresponding regulations. We also reviewed, among other documents, Coast Guard, *Navigation and Vessel Inspection Circular No. 03-03, change 2: Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 Clean Air Act Section 112(r)*, EPA 550-K-11-001 (Jan. 2011); and EPA, *General Guidance on Risk Management Programs for Chemical Accident Prevention* (40 CFR part 68), EPA 555-B-04-001 (March 2009).

[10]See GAO's Duplication and Cost Savings web page for links to the 2011 to 2019 annual reports: http://www.gao.gov/duplication/overview.

CFATS program addressed concerns about potential duplication during the rulemaking process.[11]

We identified the number of facilities subject to CFATS and the other eight federal programs we reviewed by obtaining the most recent available records and information from the respective responsible agencies, if available.[12] We selected CFATS as a comparison because (1) the CFATS program worked with some of the other programs to develop its standards and (2) DHS has designated CISA, in which the CFATS program resides, as the lead component for government-wide critical infrastructure security and resilience. To compare these records of facilities subject to programs' requirements, we used statistical analysis software to identify facilities subject to CFATS and other programs' requirements or guidance by matching facility names from the eight programs with CFATS records, including addresses, and combinations of names and addresses. To assess the reliability of the data, we reviewed documentation and information about the various systems used to house the data for these programs and spoke with or received information from knowledgeable officials about the processes for the collection and maintenance of the records and their quality assurance procedures. We also reviewed the data for missing data or obvious errors, and interviewed managers of the various data systems. While the information in the data sets provided by each program was sufficiently reliable for the purposes of documenting the number of facilities subject to the programs and for

[11]See 72 Fed. Reg. 17,687 (Apr. 9, 2007).

[12]For CFATS, we obtained and analyzed facility data, as of December 2019. For MTSA-regulated facilities, we obtained and analyzed Coast Guard facility data, as of December 2019. For TSA rail security, we obtained and analyzed inspection records related to rail shippers and receivers for fiscal years 2018, 2018, and 2019. For TSA pipeline security, we obtained and analyzed data for the top 100 critical pipelines, as determined by TSA, as of February 2020. For ATF explosive materials, we obtained and analyzed licensee data, as of November 2019. For EPA's Risk Management Program, we obtained and analyzed EPA data, as of January 2020. For EPA's RCRA program, we obtained and analyzed data on Treatment, Storage, and Disposal facilities and large quantity generators of hazardous wastes, as of March 2020. For DOT hazardous materials program, we obtained and analyzed fiscal year 2019 data from the Hazardous Materials Registration System for facilities required to register.

our analyses, issues with the comparability of information in each data set exist, which are discussed in this report.[13]

We also interviewed officials from the nine programs to gain their perspectives on program alignment, as well as representatives from eight industry associations to obtain their perspectives on the effect of alignment and nonalignment on their members. We selected the eight industry associations because their membership includes facilities subject to the programs within the scope of our review and they are part of the Chemical Sector or Water and Wastewater Systems Coordinating Councils.[14] Finally, we interviewed a nongeneralizable sample of six facility owners and operators where facilities are subject to CFATS and ATF programs to obtain their perspectives on the impact of compliance with these programs and similarities and differences among them that indicate overlap, duplication, and fragmentation.[15] The information obtained from our interviews is not generalizable, but provides insights into the programs that have regulations or guidance that align with CFATS.

To evaluate the extent to which the CFATS program collaborates with other federal programs to manage or avoid unnecessary duplication and

[13]We used statistical analysis software to match facility names, addresses, and combinations to identify the number of facilities subject to CFATS and the other programs, and due to the limitations described later in this report we were able to identify some facility matches, which we identify as a minimum threshold, but there may be more.

[14]The specific methodology for selecting associations to meet with includes identifying associations, where possible or relevant, from the Chemical, Nuclear, Water and Wastewater Systems, and other Coordinating Councils established by DHS based on the 16 critical infrastructure sectors as defined by *Presidential Policy Directive/PPD- 21: Critical Infrastructure Security and Resilience*, released on February 12, 2013. These 16 critical infrastructure sectors have assets, systems, and networks, whether physical or virtual, that are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Each sector has a self-organized and self-governed Coordinating Council that enables 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.

[15]We conducted interviews on the phone because of impacts to government operations related to Coronavirus Disease (COVID-19). While we interviewed six owners and operators where CFATS program standards and ATF requirements apply, due to COVID-19 impacts, we were not able to interview facility owners and operators subject to other programs including MTSA, Risk Management Program, and TSA. We identified potential facilities to interview based on the results of our analysis of CFATS and ATF facility records, and worked with an association to obtain contact information for the facilities.

fragmentation, we took a number of steps. First, we reviewed a May 2014 report co-authored by DHS that identified federal actions to enhance federal agency coordination and information sharing.[16] We verified with officials from CFATS and other programs within our scope that this report and related documents were intended to improve coordination, and obtained an updated interagency collaborative agreement signed in late calendar year 2018.[17]

Second, we assessed these reports, data, documents, and subsequent CFATS program actions against the applicable provisions of Executive Order 13650–*Improving Chemical Facility Safety and Security* provisions, such as the order's requirement that the working group identify areas where joint collaborative programs can be developed or enhanced, including by better integrating existing authorities, jurisdictional responsibilities, and regulatory programs in order to achieve a more comprehensive engagement on chemical risk management. In addition, we compared DHS and working group actions with the DHS *National Infrastructure Protection Plan*,[18] which establishes a framework for critical infrastructure partners, including federal agencies, to understand how critical infrastructure protection, such as chemical security, is being conducted, build upon best practices, and to identify duplicative efforts and gaps across jurisdictions.

Third, the information and communication component of internal control was significant to this objective, along with the underlying principles that management identifies, obtains from relevant internal and external sources, and uses quality information in an iterative and ongoing process, to internally and externally communicate the necessity of quality information. We assessed the agencies' policies and procedures for

[16]*Actions to Improve Chemical Facility Safety and Security—A Shared Commitment*, Report for the President (May 2014). See Exec. Order No. 13,650, 78 Fed. Reg. at 48,029, § 2(c) (directing the submission of a status report within 270 days of the date of the Executive Order).

[17]Because actions intended to achieve improved coordination may require actions to be taken by multiple agencies, while the focus of our review was on the CFATS program, we note throughout that some actions may be necessary by partner agencies in order for the CFATS program to improve collecting and sharing information.

[18]DHS, *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). PPD-21 and the NIPP also call for other federal departments and agencies to play a key role in CI security and resilience activities.

controlling relevant information from internal and external sources and using such information to make informed decisions. Specifically, we compared DHS and working group partner actions against our *Standards for Internal Control for the Federal Government*, which emphasizes the importance of quality information for management to make informed decisions, including the use of relevant data from reliable sources collected through an iterative and ongoing process.[19] Finally, we conducted structured interviews with each of the nine programs on the extent and effectiveness of coordination with CFATS. Additional details of our scope and methodology are included in appendix I.

We conducted this performance audit from February 2020 to January 2021 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

CFATS and Other Federal Programs for Chemical Safety and Security

The CFATS program is intended to ensure the security of the nation's chemical infrastructure by identifying high-risk chemical facilities, assessing the risk posed by them, and requiring implementation of

[19]*Standards for Internal Control in the Federal Government* directs managers to use quality information to achieve program objectives, where "quality" means, among other characteristics, current, complete, and accurate. GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014) In addition, DHS's Information Quality Guidelines state that all DHS component agencies should treat information quality as integral to every step of the development of information, including creation, collection, maintenance, and dissemination. The DHS guidelines also state that agencies should substantiate the quality of the information disseminated through documentation or other appropriate means. Department of Homeland Security, Information Quality Guidelines, (Washington, D.C.: Mar. 2011).

measures to protect them.[20] According to DHS, facilities that manufacture, store, ship, or otherwise use chemicals of interest above certain threshold quantities and concentrations are generally subject to CFATS reporting requirements.[21] Facilities that are determined to be high-risk must implement security measures that meet risk-based performance standards. Table 1 describes the 18 CFATS risk-based performance standards.

Table 1: Chemical Facility Anti-Terrorism Standards (CFATS) Program Standards and Descriptions

CFATS program standard	Description of CFATS program standard
1. Restrict area perimeter	Facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting.
2. Secure site assets	Facilities must secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion-detection systems.
3. Screen and control access	Facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles.
4. Deter, detect, and delay	Facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces.
5. Shipping, receipt, and storage	Facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of the quantity and physical location of hazmat.

[20]These facilities are to complete an online survey. The survey, known as a "Top-Screen," requires a facility to provide DHS with various data, including the name and location of the facility and the chemicals, quantities, and storage conditions at the site. CISA uses a risk-based approach to evaluate chemical facilities of interest that are required to report under CFATS and determine whether these facilities are high-risk and therefore subject to further requirements under the regulation. If DHS officials determine that a facility is high-risk, the facility must then complete and submit a security vulnerability assessment and site security plan that describe the existing and planned security measures to be implemented to be in compliance with the applicable risk-based performance standards. The CFATS program received over $1 billion in appropriations from fiscal year 2007 through fiscal year 2020, according to DHS.

[21]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 chemicals, 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).

CFATS program standard	Description of CFATS program standard
6. Theft and diversion	Facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures may include inventory controls, procedural measures such as access restrictions, and physical measures such as locks.
7. Sabotage	Facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures.
8. Cyber	Facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training.
9. Response	Facilities must develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.
10. Monitoring	Facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions.
11. Training	Facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders.
12. Employee background checks	Facilities must perform appropriate background checks for facility personnel and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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.
13. Elevated threats	Facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government.
14. Specific threats, vulnerabilities, or risks	Facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment, by, among other things, using new information and increasing security measures.
15. Reporting of significant security incidents	Facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities.
16. Significant security incidents and suspicious activities	Facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this CFATS standard.
17. Officials and organization	Facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan.
18. Records	Facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request.

Source: 6 C.F.R. § 27.230 | GAO-21-12

The body of federal programs applicable to chemical safety and security has evolved over time, as the statutes authorizing these regulations have been enacted and amended to address different risks. Several federal departments and agencies administer these programs, including DHS, EPA, the Departments of Justice, Labor, and Transportation. The authorizing statutes generally direct the department or agency to issue regulations intended to attain specific statutory objectives. For example, many federal programs applicable to chemical facilities primarily focus on risks to workers, public safety, human health, and the environment that may originate within a facility as a consequence of how chemicals are used or managed. Other federal programs focus on security and safety when transporting chemicals.[22] Although some actions that facilities take pursuant to one program may share similarities with, or have similar benefits as, actions that they take under another program, the purposes of the programs may be fundamentally different. The CFATS program is a more recent development within this broad regulatory framework and is the only federal program that focuses exclusively on the chemical security risks of a facility to external and insider threats. Figure 1 shows a chemical facility's storage tanks that could be subject to one or more federal programs.

[22]For example, DOT also regulates the safety and security of liquefied natural gas transportation and storage under 49 C.F.R. part 193. Because the program focused on only one chemical common to the CFATS program—methane, we did not include this program in the scope of our review.

Figure 1: Chemical Facility Storage Tanks

Source: Department of Homeland Security. | GAO-21-12

Some of the authorizing statutes and regulations, including those for CFATS, exclude facilities subject to other regulatory programs, which may prevent potential overlap, duplication, fragmentation, or conflicting requirements. The CFATS statute specifically excludes all facilities defined as a public water system or wastewater treatment works, which are regulated by the EPA. The statute also excludes facilities owned or operated by the Department of Defense or Department of Energy, regulated by the Nuclear Regulatory Commission, or regulated under MTSA by the Coast Guard. These facilities, referred to as excluded facilities, are not required to complete a CFATS screening to determine their risk even if they possess a chemical of interest above the CFATS threshold, but these facilities may choose to do so and identify their applicable exclusion. DHS has a process in place to validate such exclusion claims. Table 2 provides an overview of nine federal chemical security or safety programs that address the private sector's security posture.

Table 2: Overview of Nine Selected Federal Chemical Security or Safety Programs

Entity/Program (number of facilities covered)	Program scope and enforcement
Department of Homeland Security (DHS)	
Chemical Facility Anti-Terrorism Standards (CFATS) program (around 3,400 designated high-risk out of 48,000 required to report under CFATS)	**Scope:** The purpose of the CFATS program is to assess the risk posed by chemical facilities and inspect them to ensure compliance with DHS standards. The CFATS program covers entire facilities with threshold quantities of certain chemicals and uses a risk-based approach to evaluate chemical facilities that are required to report under CFATS and determine whether these facilities are high-risk. All facilities designated as high-risk must complete and submit a security vulnerability assessment and site security plan that describes the existing and planned security measures to be implemented to be in compliance with the applicable risk-based performance standards. CFATS inspectors conduct an authorization inspection prior to approving a facility's site security plan, and once the plan is approved, conduct compliance inspections. **Enforcement**: Order to cease operations, civil penalties, or both.
U.S. Coast Guard Maritime Transportation Security Act of 2002 (MTSA) program (3,000, all of which are generally excluded facilities under CFATS.)	**Scope:** The MTSA program is designed to deter a transportation security incident, which can include protecting the nation's ports and waterways from terrorist attacks. The MTSA facility security plan program applies to, among other things, waterfront facilities handling liquefied natural gas and liquefied hazardous gas, waterfront facilities transferring oil or hazardous material in bulk, and facilities that receive cargo vessels larger than 100 gross registered tons, with some exceptions. MTSA-regulated facilities are required to, among other things, designate a facility security officer, ensure that a facility security risk assessment was conducted, and ensure that a facility security plan is approved and implemented for facilities. MTSA requires the Coast Guard to conduct annual inspections at each facility. **Enforcement:** Civil penalties.
Transportation Security Administration (TSA) rail security program[a]	**Scope:** The TSA rail security program regulates freight railroad carriers and rail operations at certain, fixed-site facilities that ship or receive (in high-threat urban areas) specified hazardous materials by rail. This program requires that regulated facilities designate rail security coordinators and report significant security concerns. The program further requires that such facilities implement chain of custody requirements to ensure a positive and secure exchange of specified hazardous materials. TSA conducts inspections of selected rail shippers and receivers operating in high threat urban areas each year. **Enforcement:** Civil penalties.
TSA Pipeline security program (More than 3,000 pipeline operators, but the top 100 represent approximately 85 percent of the energy throughput in the U.S.)	**Scope:** The TSA Pipeline Security program is designed to enhance the security preparedness of the nation's hazardous liquid and natural gas pipeline systems. The program has guidelines that address the physical security and cybersecurity of transmission and distribution pipeline systems. TSA is responsible for conducting voluntary security reviews that assess the extent to which the 100 most critical pipeline operators are following TSA's Pipeline Security Guidelines, including voluntary assessments about once every 3-5 years. **Enforcement:** Voluntary.
Department of Justice	
Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) explosive materials program (around 10,000)	**Scope:** The ATF explosive materials program regulates, through licenses and permits, the purchase, possession, storage, and transportation of explosives, and conducts inspections approximately once every 3 years. The purpose of the ATF regulations is to ensure the public safety through the safe storage of explosives in properly constructed, maintained, located, and secured containers. For facilities that possess or store regulated explosives, ATF requires certain safety precautions related to the storage of the materials, such as prescribed distances of outdoor storage containers from inhabited buildings, passenger railways, public highways, or other containers in which high explosive materials are stored. **Enforcement:** Civil and criminal penalties.

Entity/Program (number of facilities covered)	Program scope and enforcement
Environmental Protection Agency (EPA)	
America's Water Infrastructure Act program (around 10,400 public water systems, all of which are excluded under CFATS.)	**Scope:** The America's Water Infrastructure Act program requires community water systems that serve more than 3,300 people (about 7 percent of public water systems) to develop or update risk assessments and emergency response plans. The focus of the assessments and plans is the risks of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals. Further, every 5 years, these water systems must review the risk assessment and submit a recertification to EPA that the assessment has been reviewed and, if necessary, revised. EPA officials stated that they do not review the risk assessment or independently verify the voluntary security measures listed in the emergency response plans. **Enforcement**: Civil penalties.
Risk Management Program (around 12,000)	Scope: The purpose of the Risk Management Program is to prevent accidental releases of substances that can cause serious harm to the public and the environment from short-term exposures and to mitigate the severity of releases that do occur. EPA's Risk Management Program requires facilities with threshold quantities of certain potentially dangerous chemicals to develop plans that are to summarize the potential effects of accidental releases of certain chemicals, including an evaluation of the off-site effects of a worst-case release scenario and the facility's emergency response program to prevent releases and mitigate any damage. EPA may conduct periodic compliance audits of related documentation, and on-site inspections, prioritized based on risk. **Enforcement**: Notices of violation, administrative orders, monetary fines and penalties, injunctive relief, and supplemental environmental projects.
Hazardous waste management program (around 45,000 large quantity generators and around 700 treatment, storage, or hazardous waste disposal facilities)	**Scope:** The objective of EPA's Resource Conservation and Recovery Act (RCRA) hazardous waste program is to ensure that hazardous waste is managed in a manner that protects human health and the environment. The program establishes standards applicable to hazardous waste generators and owners and operators of hazardous waste treatment, storage, and disposal facilities. RCRA regulates generators based on how much hazardous waste they produce each month. Hazardous waste treatment, storage, and disposal facilities must obtain permits to provide them with the legal authority to treat, store, and dispose of hazardous waste that detail how the facility must comply with EPA regulations. RCRA mandates that EPA inspect hazardous waste treatment, storage, and disposal facilities at least every 2 years. **Enforcement:** Administrative orders, civil and criminal penalties.
Department of Transportation	
Hazardous materials transportation program (around 14,000 facilities and transporters companies)	**Scope:** The Department of Transportation hazardous materials program is generally intended to improve public safety by preventing and mitigating accidents related to hazardous materials transportation and facilitating emergency response for any such accidents. The program requires certain safeguards for certain hazardous materials (hazmat) transported in certain quantities by rail, highway, air, or water. The Department of Transportation regulates entities that offer hazmat for transport and transport hazmat. These entities are required to develop security plans and are subject to compliance inspections. **Enforcement:** Administrative orders, civil and criminal penalties.

Source: GAO analysis of federal laws and regulations as well as federal agency data and information. | GAO-21-12

[a]TSA does not maintain a list of regulated shippers, receivers, and carriers.

Chemical Facility Safety and Security Working Group

Executive Order 13650–*Improving Chemical Facility Safety and Security*—acknowledged that there are numerous federal chemical safety and security programs and called for additional measures to improve chemical facility safety and security in coordination with owners and operators. The executive order, recognizing the overlap between some of these programs, directed DHS and chemical safety and security partners—the working group—to take specific actions related to improving federal agency coordination and information sharing; modernizing policies, regulations and standards; and working with stakeholders to reduce chemical safety and security risks, among other things. In May 2014, the working group, led by DHS, EPA, and the Department of Labor, reported on actions taken in response to Executive Order 13650, findings and lessons learned, challenges, and priority actions to be completed over time.[23] The working group report established a federal action plan with milestones and time frames to improve chemical facility safety and security, which included enhancing operational coordination and improving data management. The report also detailed concerns about duplicative data collection requirements, and federal actions needed to standardize data and facility information. In 2018, DHS and EPA, among others, reaffirmed their agencies' commitment to the working group activities in a signed charter, detailing coordination with relevant agencies to coordinate information sharing, and reviewing policies and regulations associated with chemical safety and security to minimize conflicts and overlap, among other things.

[23]*Actions to Improve Chemical Facility Safety and Security—A Shared Commitment*, Report for the President (May 2014). See Exec. Order No. 13650, 78 Fed. Reg. at 48,029, § 2(c) (directing the submission of a status report within 270 days of the date of the Executive Order).

Eight Chemical Safety and Security Programs Contain Requirements or Guidance that Indicate Some Overlap, Duplication, and Fragmentation with CFATS

We found that eight federal programs addressing chemical safety or security contain requirements or guidance that generally align with at least half of the CFATS program standards, indicating some overlap, duplication, and fragmentation between the eight programs and CFATS (CFATS is the ninth program in our review). Six of the programs regulate facilities that are not excluded under CFATS regulations, meaning that facilities regulated both by another such program and by CFATS must engage in activities to demonstrate they meet the requirements of the other program and CFATS requirements that, in some cases, may be duplicative. Certain facilities regulated by three of the programs are excluded under CFATS regulations, meaning that certain facilities regulated by these programs do not need to also adhere to CFATS requirements, but there may be fragmentation among all eight programs and CFATS.[24]

Eight Chemical Safety and Security Programs Contain Requirements or Guidance that Indicate Some Overlap with CFATS, but Some Programs Target Different Facilities

We found instances of overlapping programs engaging in similar activities and targeting similar but not necessarily the same beneficiaries (i.e., not the same facilities). Overlap occurs when multiple programs have similar goals, engage in similar activities or strategies to achieve those goals, or target similar beneficiaries.[25] All eight programs we reviewed address chemical safety and security (i.e., have similar goals), and contain requirements or guidance that generally align (i.e., engage in similar activities) with six of 18 CFATS standards regarding restricting area perimeter; securing site assets; screening and controlling access; deterring, detecting, and delaying an attack; deterring theft and diversion, and deterring insider sabotage. Specifically, the DOT hazardous materials program, MTSA program, and TSA Pipeline Security Program contain requirements or guidance that generally align with all, or almost all, of the CFATS standards. ATF's explosive materials program and TSA's rail security program contain requirements or guidance that generally align with 11 of 18 CFATS standards. Three EPA programs contain requirements or guidance that generally align with 10 to 13 CFATS

[24]The Risk Management Program regulates some facilities that may also be regulated by CFATS, as discussed later, and it also regulates public water systems and wastewater works, which are excluded under CFATS.

[25]Further, we have found that program overlap can create the potential for unnecessary duplication of efforts for administering agencies, and that such duplication can waste administrative resources and confuse those subject to the programs. We have also found that understanding the relationships between programs can help identify corrective actions to reduce or better manage the negative effects of duplication and fragmentation, which we discuss later in this report. See, http://www.gao.gov/duplication/overview.

standards. Table 3 shows the extent to which programs contain requirements or guidance that generally align with CFATS standards ("X" indicates that program regulations or guidance generally align), and where multiple programs contain requirements or guidance that align with the same CFATS program standards.[26]

[26]For all eight programs, we confirmed areas of general alignment with the CFATS program regarding security measures, including whether the eight programs contain any additional requirements, guidelines, or standards related to chemical security. The Coast Guard MTSA program detailed vessel and facility security plan requirements; the other seven programs did not identify additional security measures. We considered general alignment to occur when statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take pursuant to the CFATS program standards, to include in limited circumstances. Further, we considered program requirements or guidance to generally align with CFATS when actions required or authorized under the requirements or guidance have a different purpose or goal but may have the same effect as actions taken pursuant to the CFATS standard. While we evaluated general alignment with the CFATS standards, we are not making a determination about the effectiveness of each program or the relative security of facilities regulated by each program.

Table 3: General Alignment of Eight Federal Programs' Requirements or Guidance with Chemical Facility Anti-Terrorism Standards (CFATS) Program Standards

	Explosives materials Program (ATF)	Maritime Transportation Security Act program (Coast Guard)[a]	Hazardous materials transportation program (DOT)	Resource Conservation and Recovery Act program (EPA)	Risk Management Program (EPA)	America's Water Infrastructure Act program (EPA)[b]	Pipeline Security Program (TSA)	Rail Security program (TSA)	Number of programs with the requirements or guidance that generally align with the CFATS standard
CFATS program standard									
1. Restrict area perimeter	X	X	X	X	X	X	X	X	8
2. Secure site assets	X	X	X	X	X	X	X	X	8
3. Screen and control access	X	X	X	X	X	X	X	X	8
4. Deter, detect, and delay an attack	X	X	X	X	X	X	X	X	8
5. Secure and monitor the shipping, receipt, and storage of hazardous materials	X	X	X	X	X	X	—	X	7
6. Deter theft and diversion of potentially dangerous chemicals	X	X	X	X	X	X	X	X	8
7. Deter insider sabotage	X	X	X	X	X	X	X	X	8
8. Deter cyber sabotage	—	X	—	—	—	X	X	—	3
9. Develop and exercise an emergency response plan	—	X	X	X	X	X	X	—	6

	Explosives materials Program (ATF)	Maritime Transportation Security Act program (Coast Guard)[a]	Hazardous materials transportation program (DOT)	Resource Conservation and Recovery Act program (EPA)	Risk Management Program (EPA)	America's Water Infrastructure Act program (EPA)[b]	Pipeline Security Program (TSA)	Rail Security program (TSA)	Number of programs with the requirements or guidance that generally align with the CFATS standard
10. Maintain effective monitoring, communications and warning systems	—	X	—	X	X	X	X	—	5
11. Ensure proper security training	—	X	X	—	—	—	X	—	3
12. Perform employee background checks	X	X	X	—	—	—	X	—	4
13. Escalate the level of protective measures for periods of elevated threat	—	X	X	—	—	—	X	—	3
14. Address specific threats, vulnerabilities or risks	—	X	X	—	—	—	X	—	3
15. Report significant security incidents	X	X	X	X	X	—	X	X	7
16. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities	X	X	X	X	X	—	X	X	7
17. Establish officials and an organization responsible for security	—	X	X	X	X	—	X	X	6

	Explosives materials Program (ATF)	Maritime Transportation Security Act program (Coast Guard)[a]	Hazardous materials transportation program (DOT)	Resource Conservation and Recovery Act program (EPA)	Risk Management Program (EPA)	America's Water Infrastructure Act program (EPA)[b]	Pipeline Security Program (TSA)	Rail Security program (TSA)	Number of programs with the requirements or guidance that generally align with the CFATS standard
18. Maintain appropriate security-related records	X	X	X	X	X	—	X	X	7
Number of program requirements or guidance that generally align with CFATS	**11**	**18**	**16**	**13**	**13**	**10**	**17**	**11**	**—**

Legend:
"X" indicates that the program contains requirements or guidance that generally align with the CFATS standard, to include in limited circumstances.
"—" indicates that the program does not contain requirements or guidance that align with the CFATS standard or not applicable.
ATF = Bureau of Alcohol, Tobacco, Firearms and Explosives
DHS = Department of Homeland Security
DOT = Department of Transportation
EPA = Environmental Protection Agency
TSA = Transportation Security Administration

Source: GAO analysis of America's Infrastructure Act, DHS, EPA, ATF, DOT, regulations, guidance, and other documents. | GAO-21-12

Note: We considered general alignment to occur when statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take pursuant to the CFATS program standard, to include in limited circumstances. Further, we considered program requirements or guidance to generally align with CFATS when actions required or authorized under the requirements or guidance have a different purpose or goal but may have the same effect as actions taken pursuant to the CFATS standard.

[a]Facilities subject to the Maritime Transportation Security Act of 2002 program are excluded facilities under the CFATS program.

[b]Public water systems subject to EPA's Water Infrastructure Act program are excluded facilities under the CFATS program.

As shown in Table 3, eight federal programs we examined contain requirements or guidance that generally align with some of the 18 CFATS program standards. Similarities among the requirements or guidance indicate some overlap. For example,

Hazardous materials transportation program. We found that the DOT hazardous materials transportation program contains requirements or guidance that generally align with 16 of the 18 CFATS standards.[27] For example, both programs require facilities to ensure the security of chemicals being shipped from a facility. Under CFATS, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Similarly, under the hazardous materials transportation program, shippers (i.e., facilities) are to develop a plan that must include measures to address security risks related to shipments of hazardous materials covered by the plan en route between point of origin and point of destination, including any shipments stored incidental to movement.[28]

However, there are differences between the CFATS and DOT programs, even in the areas where we found general alignment. For example, CFATS requires facilities to have an emergency response plan, whereas the DOT program only requires emergency response information to be available. Specifically, under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders. Under the hazardous materials transportation program, facilities are required to maintain emergency response information, including a description of the hazardous materials, whenever such materials are present.[29]

GAO's Duplication and Cost Savings Framework. GAO has developed a guide for analysts—including federal, state, and local auditors; congressional staff; researchers; and consultants—and policymakers—including congressional decision makers and executive branch leaders. Using this guide, analysts and policymakers can identify and evaluate instances of overlap, duplication, and fragmentation among programs:

- **Overlap** occurs when multiple programs have similar goals, engage in similar activities or strategies to achieve those goals, or target similar beneficiaries.
- **Duplication** occurs when two or more agencies or programs are engaging in the same activities or providing the same services to the same beneficiaries.
- **Fragmentation** occurs when more than one agency (or more than one organization within an agency) is involved in the same broad area of national interest and opportunities exist to improve customer service.

Analysts and policymakers can also use the guide to identify options to reduce or better manage the negative effects of fragmentation, overlap, and duplication, and evaluate the potential trade-offs and unintended consequences of these options.

Source: GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide* GAO-15-49SP (Washington, D.C.: Apr 14, 2015). | GAO-21-12

[27]Shippers (e.g., companies that could include multiple facilities) and carriers that transport certain hazardous materials are required to register with DOT. As of fiscal year 2019, there were about 14,000 shippers registered. The program requires certain facilities to develop and implement a security plan that must include an assessment of possible transportation security risks and appropriate measures to address the assessed risks. At a minimum, the security plan must address personnel security, unauthorized access, and en route security, among other things. See 49 C.F.R. § 172.802.

[28]49 C.F.R. § 172.802(a)(3).

[29]49 C.F.R. § 172.602.

Explosive materials program. We found that ATF's explosive materials program contains requirements and guidance that generally align with 11 of the 18 CFATS standards. For example, both programs require restricted areas to be secured. Under CFATS, facilities must secure and monitor restricted areas or potentially critical targets within a facility. Security measures may include, for example, physical barriers, guard forces, or intrusion-detection systems. Similarly, ATF requires explosives to be secured. According to ATF, its regulations focus solely on where explosives are stored, rather than the entire facility. In general, ATF requires that its licensees and permittees secure all explosive materials in locked structures meeting ATF-specified criteria.[30]

There are differences between the ATF and CFATS programs, even where we found general alignment. For example, under CFATS, facilities must perform appropriate background checks for facility personnel, whereas ATF regulations state that ATF investigates applicants before issuing a license or permit and conducts background checks on individuals authorized by an employer to possess explosives materials.[31] ATF requirements or guidance did not align with seven CFATS standards. For example, ATF requirements and guidance do not include a cybersecurity program, while CFATS requires facilities to take certain steps to deter cyber sabotage. Similarly, ATF does not require security training, drills, or exercises, whereas under CFATS, facilities must ensure proper security and response training, exercises, and drills of facility personnel.

Risk Management Program. We found that the EPA's Risk Management Program contains requirements or guidance that generally align with 13 of

[30]27 C.F.R. pt. 555, subpt. K. In addition to ATF requirements, ATF has published guidance on recordkeeping, storage requirements, fireworks safety and security, disaster preparedness, and heightened security letters, among other things. Where CFATS requires facilities to generally provide for a controlled perimeter, ATF does not require licensees or permittees to establish an area perimeter with restricted access. ATF requires that all explosive materials be kept in locked structures meeting ATF-specific criteria. However, in rare circumstances, ATF has approved an alternate method or procedure in which a permittee or licensee employs area perimeter security measures to provide a substantially equivalent level of security to ATF requirements.

[31]27 C.F.R. §§ 555.33, 555.49(b).

the 18 CFATS standards.[32] For example, the Risk Management Program has requirements or guidance that generally align with CFATS standards relating to securing site assets and screening and controlling assets. Under the CFATS program, facilities must control access to the facility, secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility and restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. Similarly, the Risk Management Program requires certain facilities, depending on their risk level, to develop and implement safe work practices to provide control of hazards during operations, such as control over entrances into the facility by employees.[33] EPA officials told us that this requirement is designed to secure assets in a manner that will control chemical process hazards at facilities and to prevent inadvertent or unauthorized entry to areas with chemicals by support personnel whose jobs may not require such access. Notably, Risk Management Program regulations were not designed to prevent release incidents caused by criminal activity, according to EPA officials. Nevertheless, certain regulations may have the benefit of enhancing security and improving response to security-related incidents.

Risk Management Program requirements or guidance that generally align with CFATS program standards may still have differences from the CFATS standards.[34] For example, CFATS requires facilities to comprehensively address insider sabotage, whereas the Risk Management Program requires facilities to implement safe work practices that may have the added benefit of preventing sabotage. Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks,

[32]According to our analysis, Risk Management Program requirements or guidance that generally align with eight of the 13 CFATS program standards only apply to the highest risk facilities, which comprise about 7,000 of the 12,000 Risk Management Program-regulated facilities. We considered general alignment to occur when statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take pursuant to the CFATS standards, to include in limited circumstances.

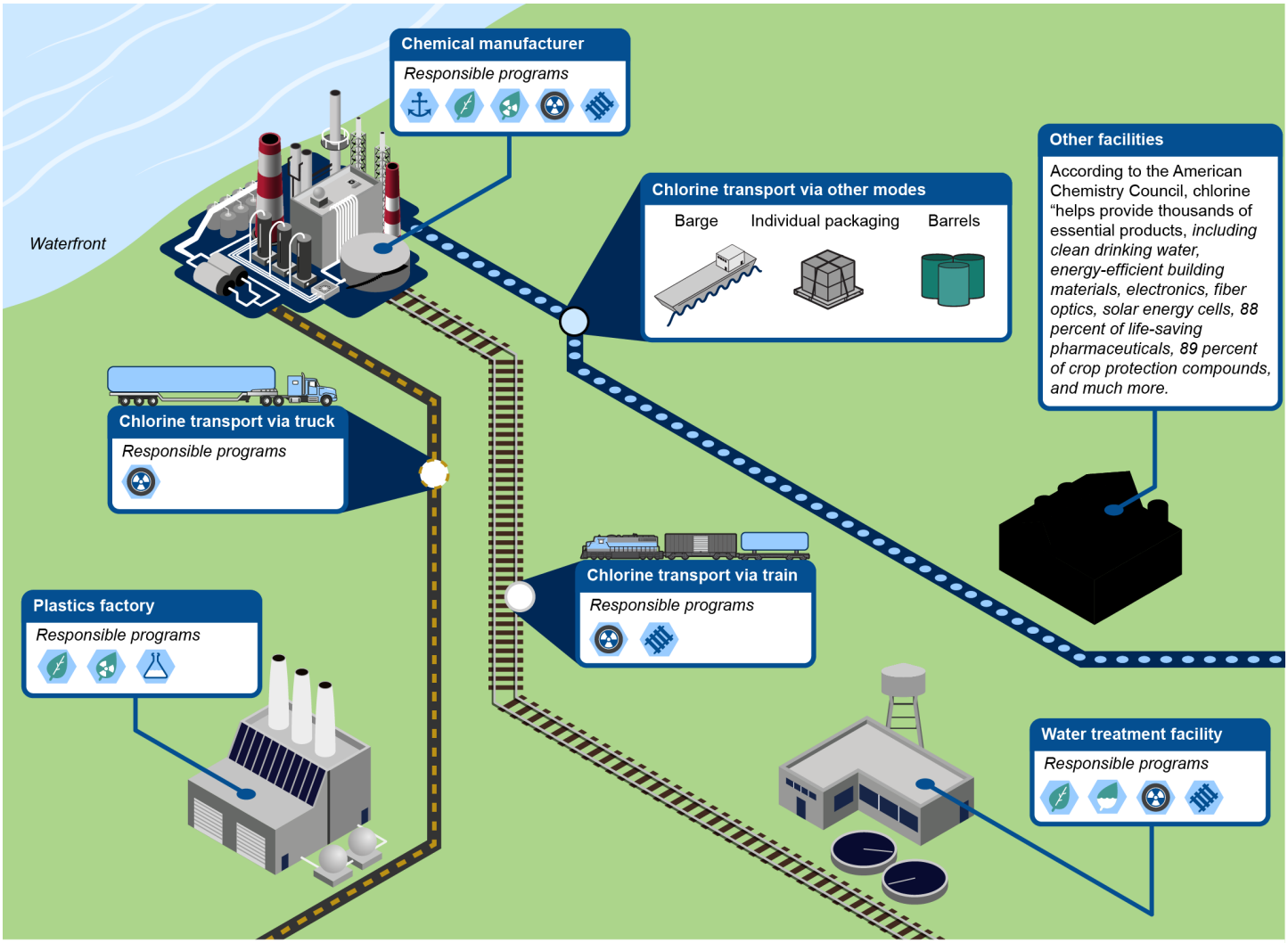
[33]40 C.F.R. § 68.69(d). According to our analysis, this Risk Management Program requirement generally aligns with six CFATS standards—restrict area perimeter; secure site assets; screen and control access; deter, detect, and delay; theft and diversion; and sabotage.

[34]The Risk Management Program regulates certain public water system and wastewater treatment works, which are excluded facilities under CFATS, and it also regulates other types of facilities that are not excluded under CFATS.

visitor controls, and restriction of access to certain areas of the facility through physical security measures, and cybersecurity measures. While the Risk Management Program includes a requirement intended to prevent inadvertent or unauthorized entry, the program does not require the other measures that might be used to meet the CFATS standard. Figure 2 shows that some facilities with, or transporters of, chlorine, a chemical regulated by multiple programs including CFATS, are subject to one or more programs where there is some overlap among requirements or guidance, including facilities subject to CFATS standards and facilities exempted under CFATS but subject to different programs.[35]

[35]Figure does not show ATF explosive materials or TSA Pipeline Security regulations.

Figure 2: Examples of Programs Applicable to Facilities with or Transporters of Chlorine Where Some Requirements or Guidance Align with Chemical Facility Anti-Terrorism Standards



Source: GAO analysis of DHS, DOT, and EPA data and information. | GAO-21-12

Note: The facilities used to illustrate some overlap among the programs covering them are actual facilities subject to the identified federal programs. However, the connections between them are illustrative.

The MTSA, RCRA, Water Infrastructure Act, and TSA rail and pipeline programs also contain requirements or guidance that generally align with CFATS standards to varying degrees, although there are differences between CFATS and these other programs. See Appendix II for our assessment of the extent to which the eight federal programs we assessed contain requirements or guidance that generally align with CFATS program standards.

Six Federal Programs' Requirements or Guidance Indicate Some Duplication with CFATS

We found that six federal programs have requirements or guidance that generally align closely enough with CFATS that facilities subject to them can use the same security measures or documentation to meet their requirements at the same facilities—if facility personnel are aware of the ability to use that information, which we discuss later in this report.[36] Duplication occurs when two or more agencies or programs engage in the same activities or provide the same services to the same beneficiaries. At least 550 of 3,300 facilities (around 16 percent) subject to the CFATS program are also subject to other federal programs we reviewed and may be able to meet some CFATS program standards by providing the CFATS program with information about measures they implemented for other federal programs. For example, we found that of approximately 3,300 high-risk facilities covered by CFATS, according to agencies' records, at least 75 are also ATF permittees or licensees, 200 facilities are also regulated by the Risk Management Program, and 250 facilities

[36]Facilities subject to three programs with overlapping requirements or guidance—Water Infrastructure Act, MTSA, and RMP, in some cases—are generally excluded facilities under CFATS.

are also regulated by the RCRA program.[37] Further, 28 CFATS-regulated facilities are also subject to TSA's Pipeline Security Program, according to TSA.[38] For example:

- We found that facilities submitted documents to the CFATS program in which they referred to actions taken or information prepared for other programs. As previously discussed, ATF's explosive materials program has requirements or guidance that generally align with 11 of the 18 CFATS standards.[39] Our analysis of CFATS records from all three facilities we interviewed that are subject to both CFATS and ATF programs found that the facilities referred to actions taken pursuant to the ATF program to meet, at least in part, the CFATS program standards for securing site assets, reporting significant security incidents, and conducting background checks. Notably, we found that there are at least 75 facilities subject to both programs, and those facilities may be able to submit information about actions taken

[37]These instances of facilities subject to CFATS and other programs are minimum numbers due to data comparability issues. We attempted to compare data from each of the nine programs to determine the extent of facilities subject to multiple programs. However, we were unable to fully validate the results of this comparison because of differences in the way data about these activities were captured and maintained in various systems. To conduct this comparison, we used a statistical software program and manual data matching to compare data on facilities across the nine programs. Using the available data, we compared more than 48,000 records of facilities that completed a CFATS Top Screen, of which around 3,300 are designated as high-risk by the CFATS program, and records from other programs in our scope based on name and location, as no unique numeric identifiers were available. Our analysis showed that the various data sets did not share common formats or defined data standards that would enable us to identify or confirm matches across sets. For example, similar to the 2014 working group report findings, we found inconsistencies. We found instances where facility names under one program may be XYZ, whereas facility names under a different program may be XYZ, Inc. Such differences make evaluating the extent of facilities subject to multiple programs challenging. Officials representing the various programs acknowledged that they have encountered challenges with the consistency of records across the programs, and described potential workarounds they can take going forward, such as manually identifying facilities subject to multiple programs.

[38]We could not match records from TSA pipelines and DOT hazardous materials programs due to differences in the way the data, such as facility names, were captured and maintained by these programs.

[39]For example, ATF investigates applicants before granting a permit or license and conducts background checks on responsible persons and employees who are authorized to possess explosives. Under CFATS, facilities must perform appropriate background checks for facility personnel and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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.

pursuant to the ATF program as part of their effort to meet certain CFATS standards.

- Similarly, we found instances where the CFATS program standard was met when facilities described the training requirements they implemented to comply with DOT training requirements. According to representatives from one association, the CFATS program accepts training programs developed pursuant to the DOT hazardous materials program to meet its standards.[40] Under CFATS, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. Under the DOT hazardous materials program, regulated facilities must train employees whose employment directly affects hazardous materials transportation safety to recognize and respond to possible security threats, and facilities must train certain employees concerning the facility security plan and its implementation.[41] Such training must include company security objectives, organizational security structure, specific security procedures, specific security duties and specific actions to be taken in the event of a security breach.

Duplication among some programs is not a new concern; in 2013, Executive Order 13650 stated that the federal government has developed and implemented numerous programs aimed at reducing the safety risks and security risks associated with hazardous chemicals. CFATS program officials acknowledge similarities among these requirements or guidance and told us that the CFATS program allows facilities to meet CFATS program standards by providing information they prepared for other programs. Specifically, facilities can describe actions they take to comply with other programs in CFATS program documentation, such as Site Security Plans.

[40]Because of impacts to government operations related to COVID-19, while we interviewed six owners and operators where CFATS program standards and ATF requirements apply, we were not able to interview facility owners and operators subject to other programs.

[41]49 C.F.R. § 172.704(a)(4), (5).

Eight Federal Programs' Similarities and Differences with CFATS Indicate Some Fragmentation

Based on our analysis of federal programs that address chemical safety and security, similarities and differences among requirements or guidance applied by various programs indicate some fragmentation among the eight federal programs and CFATS. Fragmentation occurs when more than one agency (or more than one organization within an agency) is involved in the same broad area of national interest and opportunities exist to improve customer service.

Certain facilities regulated by three of the programs are excluded from the CFATS program but have threshold quantities of chemicals of interest and would otherwise be required to meet CFATS standards.[42] For example, there are about 150,000 public water systems and over 25,000 wastewater treatment works that are excluded from the CFATS program, according to EPA's data. We have previously reported that the Water Infrastructure Act program and Risk Management Program are the key federal programs that contain requirements or guidance that that may have security benefits for public water systems and wastewater treatment works, and that more than 1,600 of these facilities that have threshold quantities of CFATS chemicals of interest are subject to the Risk Management Program.[43]

Differences in the applicable program requirements or guidance related to security for facilities that possess similar types and quantities of chemicals results in fragmentation among these programs. Facilities are often subject to multiple regulatory programs, and more than 1,100 public water system facilities regulated by the Risk Management Program are also generally regulated by the Water Infrastructure Act program, according to EPA officials. The Risk Management Program and the Water Infrastructure Act program collectively do not contain requirements or guidance that align with four CFATS standards. These are (1) security training; (2) employee background checks; (3) specific threats, vulnerabilities, or risks that are new or may not have been previously identified; or (4) escalating the level of protective measures for periods of elevated threats. According to DHS, public water systems and wastewater treatment work facilities are frequently subject to safety regulations that may have some tangential security value. However,

[42]See GAO, *Chemical Security: DHS Could Use Available Data to Better Plan Outreach to Facilities Excluded from Anti-Terrorism Standards,* GAO-20-722 (Washington, D.C.: Sep 29, 2020).

[43]See GAO-20-722. Some of these facilities are also subject to EPA's America's Water Infrastructure Act program.

according to the department, in most cases, these facilities are not required to implement security measures commensurate to their level of security risk.

In addition, approximately 3,000 facilities are excluded from the CFATS program but are regulated by the Coast Guard's MTSA program. The MTSA program contains requirements that generally align with all 18 CFATS standards, and officials from both agencies emphasized effective coordination between their programs from the moment the CFATS program was established. Officials noted that the CFATS program is modeled after the MTSA program, thus the general alignment of program requirements, and positive collaboration to manage fragmentation. Furthermore, while the CFATS and MTSA programs generally do not apply to the same facilities,[44] according to CFATS officials, coordination with the Coast Guard to harmonize efforts carried out by the CFATS program have included a staff member from the Coast Guard being on detail to the CFATS program.[45] This coordination enhanced collaboration and operational effectiveness through sharing of lessons learned from the Coast Guard regarding the MTSA program to the CFATS program, coordination on joint outreach to facilities with chemicals, and efforts to validate exclusions claimed by some facilities subject to the MTSA program. CFATS program officials also emphasized that coordination enhanced field operations by allowing CFATS inspectors to more effectively reach the appropriate MTSA program officials.

Fragmentation also occurs between programs that focus on transportation and those that focus on facilities. For example, the DOT hazardous materials program, TSA rail security program, and TSA pipeline security program have requirements or guidance for facilities as well as for transportation entities, such as rail carriers. However, CFATS only applies to facilities and the program is only responsible for a rail car when the car is within a facility, whereas TSA's authority focuses on the rail cars and the areas in which the rail cars are kept, rather than the facilities as a whole. As a result, transportation entities are subject to

[44]Our analysis of CFATS and MTSA facility information identified four facilities that are subject to both CFATS and MTSA programs, out of more than 3,300 subject to CFATS and around 3,000 subject to MTSA. These are referred to as "parsed" facilities by the CFATS and MTSA programs, and generally indicate a geographical division at the facility, such as a road, that the programs and facilities have agreed upon and that divides the parts of the facilities to which the different programs apply.

[45]CFATS and MTSA program officials told us that the position was eliminated due to resource constraints.

different requirements or guidance regarding chemical security than are facilities that are also subject to CFATS.

Representatives from the eight industry associations we met with described mixed views on the effect of fragmentation among chemical safety and security programs. For example, representatives from one association stated that DOT regulations and CFATS regulations generally cover different aspects of chemical security. That is, DOT regulations cover the transportation of chemicals and CFATS regulations come into play when the chemicals arrive at a facility (see fig. 1 above). However, representatives from three of these associations also noted that regulating agencies could better coordinate in certain areas, which we discuss later in this report. For example, one association highlighted similarities among the programs that achieve some benefits, such as when a chemical facility installs a berm on site to prevent chemicals from leaking out into the environment, and that berm also prevents a malicious actor from driving a vehicle onto the property. The berm is primarily in place for environmental protection, and such measures are not a substitute for security programs like CFATS and MTSA and do not require the same level of security, but they also create a security benefit, according to this association.

Chemical Safety and Security Programs Could Further Improve Information Sharing and Modernize Policies

CFATS and other federal programs have opportunities to improve information collection and sharing, as well as further modernizing policies, standards, and regulations. Executive Order 13650 directed the CFATS program and chemical safety and security partners to establish a working group to take actions focused on, among other things, (1) modernizing policies, regulations, and standards; (2) improving coordination; and (3) enhancing information collection and sharing. While the partners formed a working group that has generally taken steps pursuant to the executive order, including modernizing some policies and improving certain aspects of coordinating, there remain opportunities for CFATS and other federal programs to further enhance information collection and sharing, and to take additional steps to modernize policies, standards, and regulations by identifying security gaps.

Chemical Safety and Security Partners Established a Working Group and Have Coordinated and Shared Some Information

In response to the August 2013 Executive Order 13650, the chemical safety and security partners established a working group. In 2014, the working group issued a report that described the steps it needed to take to enhance coordination and information sharing. The report also described actions the working group planned to take to enhance coordination and information sharing, among other things. Subsequently, the working group took some steps to modernize policies, regulations and standards, as well as improve coordination.

Chemical Facility Anti-Terrorism Standards (CFATS) Overarching Security Objectives. The Department of Homeland Security has grouped the 18 CFATS standards into five security objectives:

1. **Detection**: covers portions of standards 1-7 (Restrict area perimeter; Secure site assets, Screen and control access; Deter, detect, and delay an attack; Secure and monitor the shipping, receipt, and storage of hazardous materials; Deter theft and diversion of potentially dangerous materials; Deter insider sabotage)
2. **Delay:** covers portions of standards 1-7 (Restrict area perimeter; Secure site assets, Screen and control access; Deter, detect, and delay an attack; Secure and monitor the shipping, receipt, and storage of hazardous materials; Deter theft and diversion of potentially dangerous materials; Deter insider sabotage)
3. **Response:** covers portions of standards 9, 11, 13, and 14 (Develop and exercise an emergency response plan; Ensure proper security training; Escalate the level of protective measures for periods of elevated threats; Address specific threats, vulnerabilities, or risks)
4. **Cybersecurity:** covers standard 8 (Deter cyber sabotage)
5. **Security Management**: covers portions of standards 10-12, and 15-18 (Maintain effective monitoring, communications and warning systems; Ensure proper security training; Perform employee background checks; Identify and investigate significant security incidents and suspicious activities; Establish officials and an organization responsible for security; Maintain appropriate security-related records).

Source: GAO analysis of Department of Homeland Security documentation. | GAO-21-12

Modernizing policies, regulations, and standards. Since 2014, the working group members have taken some actions to modernize policies and regulations, including engaging in rulemaking, sending out requests for information, issuing an advisory, and publishing some new guidance. Collectively, the working group established regional operating procedures for chemical safety and security partners, including plans for joint outreach to facilities, coordinated inspections, and information sharing. Individual working group members also took some steps to modernize policies, regulations and guidance. For example, the EPA made amendments to the Risk Management Program regulation and, together

with the Department of Labor and ATF, published an advisory for ammonium nitrate accident prevention.[46]

Likewise, the CFATS program has matured, and according to program managers, so too have the programs' policies for evaluating compliance with its 18 CFATS standards. For example, according to DHS officials, the program has recognized that CFATS standards are not necessarily discrete security standards. Instead, the CFATS program has grouped its standards into five security objectives—detection, delay, response, cybersecurity, and security management (see sidebar). According to a program official, the CFATS program looks collectively at a facility's efforts to improve its security posture, noting that not all standards necessarily apply to all facilities. As a result, CFATS developed a holistic approach that aimed to take a collective look at each facility and its efforts to improve its security posture, and developed the security objectives, which is indicative of CFATS' general flexibility in determining compliance with the CFATS standards. The security objectives are subsequently used when reviewing each facility, instead of reviewing and tracking every CFATS standard in isolation. For example, according to the CFATS official, requiring a perimeter fence is not going to be helpful or make sense for a university that must comply with the CFATS standard on restricting area perimeter.

Improving coordination. The CFATS program and working group partners have taken steps to enhance federal agency coordination. For example, in 2018, DHS, EPA, and representatives from ATF and DOT, reaffirmed their agencies' commitment to the working group activities in a signed charter, detailing recurring meetings, coordination and information sharing, and reviewing policies and regulations associated with chemical safety and security to minimize conflicts and overlap, among other things. Our analysis of interagency agreements and interviews with program officials confirmed that, as of June 2020, there is some continued coordination between CFATS and eight programs. For example, officials from the CFATS program and working group partners reported that they coordinate through regular meetings or working groups on chemical safety and security. Program officials from six of eight programs reported that their coordination with CFATS was either very or moderately

[46]See, *Chemical Advisory: Safe Storage, Handling, and Management of Solid Ammonium Nitrate Prills*, EPA 550-F-15-001, issued June 2015, as part of a federal effort to improve chemical risk management.

effective.[47] Officials from the CFATS program and EPA said they meet monthly, and despite their differing purposes, their common interest in chemical safety and security encourages even more coordination on an ad hoc basis. For example, officials described outreach to law enforcement and first responders, as well as safety training.

Our analysis of chemical safety and security regional operating procedures found that they call for, among other things, coordinated outreach and inspections at facilities subject to overlapping programs. All 10 regional operating procedures address coordinating inspections, conducting joint inspections, inviting other programs to inspections, and sharing lists of the facilities they regulate. For example, officials from CFATS and EPA's Risk Management Program told us that ongoing interagency coordination helps their programs manage instances of potential overlap among the programs.[48]

Industry associations also stated that some effective coordination takes place. For example, according to an association representative we interviewed, DOT allows facilities to incorporate its hazardous materials transportation requirements into facility security plans that are required for MTSA and CFATS. Another association representative recognized that each program has a different purpose and that overlap among the programs provides an opportunity for programs to collaborate regarding actions facilities can take to meet multiple programs' requirements, such as by reusing actions taken or information prepared. For example, DOT and the CFATS program coordinate well because DOT regulations cover the transportation of chemicals and CFATS takes over when the chemicals arrive at the facility.

[47]Program officials from the Water Infrastructure Act and RCRA programs reported no opinion or that no coordination takes place.

[48]Facilities holding more than a threshold quantity of a regulated hazardous substance in a process are required to comply with EPA's Risk Management Program regulations depending on their risk level. As a result, different facilities covered by the regulations may have different requirements depending on their processes. A facility can have multiple regulated processes, which can be classified under different Risk Management Program levels. Program Level 1 has the least stringent requirements of the three levels, whereas Program Level 3 has the most stringent requirements. 40 C.F.R. § 68.10. EPA regulations define process as any activity involving a regulated substance, including any use, storage, manufacturing, handling, or on-site movement of such substances, or combination of these activities. 40 C.F.R. § 68.3.

Chemical Safety and Security Partners Have Not Identified the Extent of Duplication, Clarified What Information Can Be Reused From Programs with Overlapping Requirements, or Assessed Potential Security Gaps

While the partners have generally identified opportunities to modernize policies and improve certain aspects of coordinating, they could further enhance information collection and sharing and further modernize policies, standards, and regulations, as called for in Executive Order 13650—such as by identifying and closing potential security gaps. Specifically, regarding opportunities to improve information collection and sharing, we found that chemical safety and security programs have not identified the extent of overlap or duplication, and some facilities may be unnecessarily developing duplicative information. Regarding modernizing policies, standards, and regulations, we found that DHS and the EPA have not collaborated to identify potential security gaps at water facilities.

Chemical safety and security programs have not identified the extent of duplication with facilities subject to overlapping requirements or guidance

The CFATS program and partners with chemical safety and security programs are not always aware of the extent to which facilities subject to their programs are covered by other programs, including the requirements and guidance of such programs, and the extent of overlap, duplication, and fragmentation among them. In prior work, we have found that program overlap can create the potential for unnecessary duplication of efforts for administering agencies, and that such duplication can waste administrative resources and confuse those subject to the programs. We have also found that understanding the relationships between programs can help identify corrective actions to reduce or better manage the negative effects of duplication and fragmentation.[49] These nine programs collectively do not have current, complete, and accurate information about facilities subject to their programs—a necessary first step to identify the extent of overlap and duplication to be managed. As described above, we identified at least 550 of 3,300 facilities (around 16 percent) subject to the CFATS program are also subject to other federal programs we reviewed. However, we were unable to fully validate the results of this comparison because of differences in the way programs capture and maintain data about these activities in their various systems.

CFATS and other programs took steps to compare facility information, but the efforts did not yield conclusive results. Specifically, in 2013, the

[49]We have previously reported that fully addressing issues of fragmentation, overlap, and duplication is challenging, as they may involve long-standing programs with entrenched constituencies. The lack of comprehensive and reliable data on the number, cost, and performance of federal programs compounds these challenges. See GAO's Duplication and Cost Savings web page for links to the 2011 to 2019 annual reports: http://www.gao.gov/duplication/overview.

CFATS program coordinated with other DHS and federal programs that address chemical safety and security to evaluate the extent of facilities subject to overlapping program requirements as part of its response to Executive Order 13650. In their 2014 working group report, the chemical safety and security partners populated EPA's Facility Registry System with information aggregated from several chemical regulatory programs, including CFATS, as a one-time effort to match facilities subject to the multiple programs. However, chemical safety and security partners have different understandings of the status of working group efforts to address inconsistent program terminology, records, and facility naming conventions, among other things, that would be beneficial for identifying facilities covered by multiple programs.

For example, CFATS program officials consider facility matching to be an ongoing effort that includes assigning unique EPA identifiers to CFATS records, but other programs' officials, including those managed by EPA, told us that CFATS provided data approximately six years ago as a customized data retrieval, one time. CFATS program officials further noted that the facilities, not the programs, populate all facility records related to their name, location, and other identifying information, and the CFATS program does not have control over how these private companies maintain their records. The CFATS program also had concerns that sensitive CFATS information would not be subject to the same security protocols if entered into other agencies' systems.[50]

Nevertheless, the chemical safety and security working group conducted matching of records in 2014, and noted that, for example, around 30 facilities were known to be subject to the CFATS program and ATF requirements for explosive materials. As described earlier, we identified at least 75 facilities subject to both the ATF and CFATS programs. While the report detailed the benefits of developing common terminology to facilitate information sharing and use, it focused on identifying noncompliant facilities and sharing information with first responders, not on identifying facilities subject to overlapping programs with some duplicative requirements.

[50]CFATS records are protected by a special security category, but the CFATS program offers partner agencies training in how to properly secure and handle such records.

Industry representatives we interviewed provided perspectives on how enhanced understanding among chemical programs of which facilities are covered by which programs would be useful for a variety of reasons.

- Representatives we interviewed from six facilities that are subject to CFATS and ATF program requirements all indicated that conducting this type of evaluation on a more regular basis would be beneficial. For example, as previously noted, one facility representative stated that because the CFATS program duplicates some efforts of ATF, a challenge was having to create a new document for CFATS with the same information they already provide to other programs. Representatives from another facility subject to CFATS and ATF programs told us that because the CFATS program asked for the same information they already provide to ATF, they had met CFATS program standards through responses that described the exact same processes they follow for ATF. Officials from the CFATS program told us that they do their best to accept documents and procedures developed for other programs, as appropriate.
- Facility leaders at four of six facilities we met with that are subject to CFATS and ATF programs told us improved program coordination would be beneficial; such collaboration could help manage instances of overlap, duplication, and fragmentation among chemical safety and security programs. For example, one facility representative said it would be helpful if the CFATS program considered whether an ATF inspection might suffice for the CFATS program, or at least be coordinated. Another facility representative told us that some programs do not recognize that CFATS-approved security plans contain the same information they use to comply with other programs' security planning requirements, and instead require the facility to recreate documents.
- Representatives from three of eight industry associations we interviewed told us that there is some interagency coordination among chemical safety and security programs, but agencies could better coordinate to address overlapping requirements. For example, representatives observed that inspections are not coordinated, even though many inspectors focus on similar aspects of the facility, such as perimeter security. Representatives praised instances where program requirement reciprocity occurs, such as instances where CFATS inspectors recognize and accept DOT hazardous materials program training requirements. Program officials expressed mixed views on the extent that coordinated outreach at facilities will address facility concerns. For example, officials from ATF's explosive materials program cautioned that coordinated inspections may not achieve the

benefits facilities want, while officials from the CFATS and MTSA programs emphasized the benefits of such coordination between their programs.

Executive Order 13650 directed the working group to take specific actions in order to enhance federal coordination regarding chemical safety and security and enhance information collection and sharing across agencies to support more informed decision-making, streamline reporting requirements, and reduce duplicative efforts. In addition, *Standards for Internal Control for the Federal Government* emphasizes the importance of quality information for management to make informed decisions, including the use of relevant data from reliable sources collected through an iterative and ongoing process.[51]

Officials from the CFATS program told us that the program is limited in actions it alone can take to improve data management, that there is no single naming structure used by partners, and that they have concerns about sharing CFATS records with other programs.[52] However, in June 2020, officials from relevant EPA programs detailed the security of their system, and how they could work with DHS to mitigate such concerns, and told us they could potentially use one of their data systems to match facilities in a coordinated effort with the CFATS program and other chemical safety and security partners.[53]

However, the CFATS program has not updated this effort since 2014, and it does not periodically evaluate the extent to which its regulated facilities are regulated by other chemical programs, that have requirements or

[51] *Standards for Internal Control in the Federal Government* directs managers to use quality information to achieve program objectives, where "quality" means, among other characteristics, current, complete, and accurate. GAO-14-704G. In addition, DHS's Information Quality Guidelines state that all DHS component agencies should treat information quality as integral to every step of the development of information, including creation, collection, maintenance, and dissemination. The DHS guidelines also state that agencies should substantiate the quality of the information disseminated through documentation or other appropriate means. Department of Homeland Security, Information Quality Guidelines, (Washington, D.C.: Mar. 2011).

[52] Because actions intended to achieve improved coordination may require actions to be taken by multiple agencies, while the focus of our review was on the CFATS program, we note throughout that some actions may be necessary by partner agencies—EPA, ATF, and DOT—in order for the CFATS program to improve collecting and sharing information.

[53] EPA officials told us the system they used in 2014 already has some information from the EPA, and that they can segment information by program to address the CFATS program concerns.

guidance that generally align with some CFATS standards. Without an iterative and ongoing process, such as collecting and sharing information across agencies that takes into account existing authorities and jurisdictional responsibilities, to identify the extent of overlap among facilities subject to CFATS and other programs, and acknowledgement of some duplication that could be better managed, the CFATS program does not have the necessary information to guide regional coordination. Moreover, the CFATS and partner programs established regional operating procedures that detail plans to coordinate across programs, such as inspections and information sharing efforts, but these efforts will be limited until the partners collect and use better information on the extent of overlap and duplication.

The CFATS program guidance does not clarify what information facilities can reuse from programs with overlapping requirements

According to CFATS program officials, facilities can reference any information prepared in accordance with other federal programs and procedures in their security plans to potentially meet CFATS program standards. However, the CFATS program has not collected and documented a list of what such information would entail, such as whether reference any information means to reuse it, reproduce it in a specific format, or demonstrate actions taken. As a result, facilities subject to CFATS may be taking unnecessarily duplicative actions because the CFATS program does not provide detail on what information they can reuse from programs that contain regulations or guidance that generally align with some CFATS standards, such as for response plans or background checks, that may satisfy the CFATS standard. Based on our analysis, some facilities with chemicals of interest are subject to multiple programs. Further, facilities subject to multiple programs may be required to develop duplicative information to demonstrate compliance with these programs for background checks and securing site assets, among other requirements. For example, facilities may be unaware that some of the actions that they take to meet other programs' requirements may also be used to meet CFATS requirements.

Our analysis of CFATS fact sheets and interviews show that the CFATS program is aware of some overlap between other programs' requirements or guidance and CFATS standards, such as ATF's explosive materials background checks and DOT hazardous materials transportation program training documents. However, the CFATS program has not disseminated information to facilities subject to the overlapping programs detailing the actions taken pursuant to other programs and information that facilities may be able to reuse that may be included in their security plans for CFATS. Instead, CFATS guidance directs facilities to request compliance assistance visits for technical assistance (i.e., help from the CFATS

program to answer specific questions about meeting its standards) to obtain the information. Moreover, the CFATS program has not clarified its internal guidance for use during assistance visits, such as by developing a list of actions taken pursuant to, or information prepared for, other programs those facilities subject to overlapping programs may be able to reuse and include in their security plans to comply with CFATS standards.

For example, one facility representative told us that the CFATS program did not accept a security plan it had prepared to meet a DOT program requirement it considered duplicative, instead requiring the facility to create a new CFATS-specific plan even though its contents were the same as those provided for other programs. DHS officials told us that they do their best to accept plans and procedures developed for other purposes as long as the details of those plans satisfy CFATS. Since the program does not have guidance, such as a list of what actions facilities may have taken pursuant to other programs and information that facilities may be able to reuse, it is unable to verify that it is systematically applying its standards to all such facilities.

Industry stakeholders stated that there were challenges in complying with multiple regulatory programs. For example, representatives from one association told us that the CFATS program's 10 regions sometimes have different interpretations of the requirements, which creates confusion and inconsistency. These views were reflected in the 2014 working group report, which stated that the industry faced challenges of complying with the requirements of the multiple agencies and programs with regulatory authority over chemical safety and security.

CFATS program officials told us that the program is performance-based, meaning that facilities can submit any information they think will meet its standards. As described earlier, the CFATS program modernized its policies in acknowledgment of CFATS' general flexibility in determining compliance with the CFATS standards, which resulted in development of the five security objectives that are now used when reviewing each facility, instead of reviewing and tracking every CFATS standard in isolation. Moreover, DHS stated in 2007 that it does not intend to require duplication of effort when facilities have implemented adequate security measures and that where there is concurrent jurisdiction, DHS will work

with other federal agencies to ensure that facilities can comply with requirements while minimizing any duplication.[54]

Concerns about overlapping and duplicative requirements and the need for CFATS program clarifying guidance are not new. During the 2007 rulemaking, several commenters raised questions about the use of other federal background checks for CFATS. In its response to those comments, DHS recognized that many facilities already perform background checks and indicated that it would consider such checks if they contained all of the required elements.[55] Also, representatives from one association told us they had advocated for a universal background check process during CFATS rulemaking in 2014.[56]

The August 2013 Executive Order 13650 directed the working group to take specific actions in order to enhance federal coordination regarding chemical safety and security and enhance information collection by and sharing across agencies to support more informed decisionmaking, streamline reporting requirements, and reduce duplicative efforts, among other things.[57] In its 2014 report to the President, the working group stated that DHS would develop best practice guidance for CFATS standards, a comprehensive regulatory fact sheet, and other information for stakeholder use in determining regulations applicable to their facilities.

[54]See 72 Fed. Reg. 17,687, 17,707, 17,719 (Apr. 9, 2007). In the preamble to the interim final rule, DHS stated that it does not intend to require duplication of effort when facilities have implemented adequate security measures. The preamble also stated that DHS is aware of the potential overlap between CFATS and existing programs, and that where there is concurrent jurisdiction DHS will work with other federal agencies to ensure that facilities can comply with requirements while minimizing any duplication, including considering formalized arrangements such as an inter-agency coordination process, to resolve jurisdictional questions or conflicts. Executive Order 13650 subsequently directed actions to, among other things, reduce duplicative efforts, but as of October 2020, the CFATS program has not entered into any such formalized arrangements to resolve jurisdictional questions and the extent of duplication, as well as gaps, remain unexamined.

[55]See 72 Fed. Reg. at 17,708-09.

[56]The Department published an Advance Notice of Proposed Rulemaking on August 18, 2014, as an initial step towards maturing the program. See 79 Fed. Reg. 48,693 (Aug. 18, 2014).

[57]Specifically, among other things, Executive Order 13650 called for the working group to identify and recommend possible changes to streamline and otherwise improve data collection to meet the needs of the public and federal, state, local, and tribal agencies, including opportunities to lessen the reporting burden on regulated industries. To the extent feasible, efforts are to minimize the duplicative collection of information while ensuring that pertinent information is shared with all key entities.

Standards for Internal Control for the Federal Government emphasizes the importance of quality information for management to make informed decisions, including the use of relevant data from reliable sources collected through an iterative and ongoing process, and communicating quality information externally.[58] Nevertheless, CFATS program officials told us they have not developed a process to identify a list of actions taken or documents prepared for other programs, such as those we identified as overlapping that contain some requirements or guidance that generally align with some CFATS standards, that can be used to meet CFATS standards. A list of commonly accepted actions that facilities may take and information that facilities may prepare in accordance with other federal program requirements, such as guidance or a fact sheet detailing such information, would help reduce the burden on the regulated community by streamlining CFATS reporting requirements and reducing duplicative efforts.

DHS and the EPA have not collaborated to modernize policies and assess potential water security gaps

Among the nine programs in our review, we found that DHS's CFATS program and the EPA's Water Infrastructure Act program and Risk Management Program have not collaborated to assess potential water security gaps. As discussed above, public water systems and wastewater treatment works are statutorily excluded facilities under the CFATS program. Water and wastewater treatment facilities may present attractive terrorist targets due to their large stores of potentially high-risk chemicals and their proximities to population centers, according to the working group's 2014 report. We reported in September 2020 that some of the approximately 150,000 public water systems and 25,000 wastewater treatment works use chemicals of interest in quantities that are at or above CFATS program thresholds, according to EPA officials and our analysis of EPA data. Specifically, we found that the Risk Management Program regulates at least 1,100 public water system and 500 wastewater treatment works facilities for many of the same chemicals at

[58]GAO-14-704G.

the same threshold quantities as the CFATS program's chemical release attack scenario.[59]

We further reported in September 2020 that the Water Infrastructure Act and the Risk Management Program are the key federal programs that contain requirements or guidance that may have security benefits for public water systems and wastewater treatment works. While the EPA programs were established by statute to address different risks and accomplish different purposes than the CFATS program, according to our analysis, the Risk Management Program and Water Infrastructure Act programs contain requirements or guidance that generally align with over half of the 18 CFATS standards, as discussed above. For example, both the Risk Management Program and the Water Infrastructure Act contain requirements or guidance that generally align with the CFATS standards regarding securing site assets and screening and controlling access. Nevertheless, there are differences that may affect the security posture of a regulated facility. For example, the Risk Management Program and Water Infrastructure Act programs do not contain requirements or guidance regarding security training or background checks. In addition, while the Water Infrastructure Act program contains guidance on cybersecurity, the Risk Management Program does not. Since wastewater treatment facilities are not subject to the Water Infrastructure

[59]The Risk Management Program risk assessment is based on a hazardous release scenario that could cause injuries or harm human health, which has a higher threshold quantity for certain regulated chemicals than the theft/diversion scenario accounted for by the CFATS program. For example, the threshold quantity for a release of chlorine under both Risk Management Program and the CFATS program is 2,500 pounds, but the threshold quantity for chlorine for a theft/diversion attack scenario under the CFATS program is 500 pounds. As a result, the number of facilities we identified is a minimum. In 2008, DHS commissioned a White Paper to identify the strategy the department could implement to regulate water and wastewater facilities under the CFATS program if the program's statutory exclusions were eliminated. DHS estimated that several thousand of these facilities had threshold quantities of CFATS chemicals of interest (for both the release and threat/diversion attack scenarios), many of which the CFATS program would categorize as high-risk. DHS updated the White Paper in 2018 to reflect changes in the way CISA determines high-risk facilities. This revision did not update the estimate of the existing number of water and wastewater facilities and the chemicals they possess. We are not reporting these estimates because, among other reasons, the data used have not been updated since 2008, and the White Paper stated that the estimates may be high because many facilities had switched away from CFATS-regulated chemicals to safer ones that are not chemicals of interest. According to water association officials, this trend has continued over the past decade.

Act program, they are generally not required to implement cyber security measures.[60]

Executive Order 13650 directs the working group—which includes both DHS and EPA—to take actions to modernize policies, standards, and regulations, such as to develop options to identify and close security gaps, to improve chemical facility safety and security through improvements to existing risk management practices. The working group report identified a planned action to work with Congress to pursue removing the statutory exclusions for water and wastewater facilities. Further, the National Infrastructure Protection Plan establishes a framework for critical infrastructure partners, including federal agencies, to understand how critical infrastructure protection, such as chemical security, is being conducted, build upon innovative methods for federal interagency collaboration regarding chemical facility safety and security, and to identify duplicative efforts and gaps across jurisdictions.

EPA program officials and representatives from associations we met with expressed mixed views on the potential for security gaps at water and wastewater treatment facilities. For example, EPA Risk Management Program and Water Infrastructure Act program officials stated that neither the Risk Management Program nor the Water Infrastructure Act program requires facilities to implement the same level of security as the CFATS program.[61] Representatives from all three of the chemical associations we met with that have members regulated by the CFATS program and the Risk Management Program agreed that the Risk Management Program does not require the same level of security as the CFATS program.

In contrast to program officials, representatives from three water associations we met with told us that in the absence of statutory

[60]Water and wastewater facilities may implement the voluntary American Water Works Association's security practices management standard, which contain elements that generally align with all 18 CFATS standards—including cybersecurity. See American National Standards Institute and American Water Works Association, *AWWA Management Standard: Security Practices for Operation and Management*. The purpose of this standard is to define the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety (including protection from acts of terrorism), and public confidence. Topics covered include security culture, defined security roles and employee expectations, vulnerability assessment, resources dedicated to security and security implementation, access control and intrusion detection, monitoring and surveillance, and information protection and continuity.

[61]The EPA programs were established by statute to address different risks and accomplish different purposes than the CFATS program.

exclusions, the CFATS program would potentially duplicate the requirements of the Risk Management Program and the Water Infrastructure Act program. For example, representatives from two of these associations stated that CFATS and the Risk Management Program both contain access control and perimeter security requirements, and the Water Infrastructure Act program requires facilities to include physical security measures in their emergency response plans. These association representatives stated that the Water Infrastructure Act's requirement to assess the risks posed by malevolent acts and include plans and procedures that can be utilized in the event of such acts in their emergency response plan aligns with several CFATS standards.

Water association representatives also noted that, in addition to complying with the EPA program requirements, water and wastewater facilities may also implement the voluntary American Water Works Association's security practices management standard. According to two of the three water associations we met with, the Risk Management Program and Water Infrastructure Act program, when combined with the voluntary standard that water and wastewater facilities may choose to implement, covers all of the CFATS standards.[62] However, according to EPA program officials, the voluntary water and wastewater standards are not as comprehensive as the CFATS program's 18 standards, and it is unclear the extent to which public water systems and wastewater treatment works implement the standard because its use is entirely voluntary.[63]

EPA and DHS senior officials have previously stated that there are security gaps at water and wastewater facilities because these facilities are excluded facilities under the CFATS program, but the relevant programs have not collaborated to address these gaps. Specifically, in 2010, the EPA Assistant Administrator testified that, among other things,

[62]The remaining water association was not familiar with all of the CFATS standards and how they might align with Risk Management Program and Water Infrastructure Act program requirements or guidance.

[63]We found that the standard contains guidance that generally align with all of the 18 CFATS standards, which include the four CFATS standards that neither the Risk Management Program nor the Water Infrastructure Act program contained. For example, the standard recommends that public water systems and wastewater treatment works facilities train employees in security awareness, individual responsibility, and appropriate responses. Further, the standard also calls for facilities to monitor available threat information and escalate security procedures in response to threats.

there is a critical gap in the U.S. chemical security regulatory framework – namely the exemption of drinking water and wastewater treatment facilities from CFATS standards.[64] In the same hearing, DHS leadership also stated that there is a critical gap in the U.S. chemical security regulatory framework—the exemption for drinking water and wastewater treatment facilities from CFATS—and stated that DHS needs to work with Congress to close this gap to secure substances of concern at these facilities.[65] According to the 2014 working group report, which both EPA and DHS senior officials signed, the regulatory programs that cover water and wastewater treatment facilities do not properly address the risks presented by chemicals.

In September 2020, CFATS and EPA officials stated that an assessment of possible security gaps has merit. According to DHS officials, the general alignment of Water Infrastructure Act requirements or guidance with some CFATS standards may not reflect the level of security achieved because, unlike the CFATS program, the Water Infrastructure Act program does not include verification measures.[66] In response to our September 2020 report, DHS stated that some facilities, such as public water systems and wastewater treatment work facilities, are frequently subject to safety regulations that may have some tangential security value. However, in most cases, these facilities are not required by law to implement security measures commensurate to their level of security risk,

[64]Peter S. Silva, Assistant Administrator for Water, Environmental Protection Agency, *Chemical Security: Assessing Progress and Charting a Path Forward,* testimony before the Senate Committee on Homeland Security and Governmental Affairs, 111th Cong., 2nd Sess., March 3, 2010.

[65]Rand Beers, Under Secretary for National Protection and Programs Directorate, Department of Homeland Security, *Chemical Security: Assessing Progress and Charting a Path Forward*, testimony before the Senate Committee on Homeland Security and Governmental Affairs, 111th Cong., 2nd Sess., March 3, 2010. The testimony also stated that DHS supports amending the exemption for drinking water and wastewater facilities to be specific that EPA would have the lead on regulating for security, with DHS supporting EPA to ensure consistency, which could be achieved, for example, by the use of CFATS compliance tools and risk analysis with modifications as necessary to reflect the uniqueness of the water sector and statutory requirements.

[66]The Water Infrastructure Act program requires a regulated public water system, every 5 years, to review its risk assessment and submit a recertification to EPA that the assessment has been reviewed and, if necessary, revised. The America's Water Infrastructure Act provides that the certification must contain only information that identifies the community water system submitting the certification, the date of the certification; and a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable. 33 U.S.C. § 300i-2(a)(4). EPA program officials stated that they do not review the risk assessment or independently verify the security measures listed in the emergency response plans.

like similar facilities regulated by other regulatory regimes, according to DHS.

According to the working group report to the President, in order to properly address the risks presented by the chemicals located at many water and wastewater treatment facilities with large stores of potentially high-risk chemicals and their close proximities to population centers, the statutory exemption from CFATS for water and wastewater treatment facilities could be removed. The report listed in the federal action plan that the working group would work with Congress to pursue action to remove the water and wastewater treatment facilities exemption from CFATS so that security at these facilities can be regulated. However, CFATS and the EPA programs have not assessed the extent of risks associated with such potential gaps, and subsequently have not developed a proposal and submitted it to the Secretary of Homeland Security, EPA Administrator, and Congress, as appropriate. EPA is the designated federal agency responsible for supporting the security and resilience of water and wastewater facilities, and DHS leads the national effort to understand and manage cyber and physical risk to U.S. critical infrastructure. By collaborating to assess the extent to which potential security gaps exist at water and wastewater facilities and proposing steps, including statutory changes, to address them, as appropriate and feasible, DHS and EPA would better ensure the security of water systems and wastewater facilities through chemical risk management.

Conclusions

Individuals intent on gaining access to or using hazardous chemicals to carry out a terrorist attack continue to pose a threat to the security of facilities that use these chemicals as well as to surrounding populations. The body of federal regulations applicable to chemical safety and security has evolved over time. Authorizing statutes and regulations implemented programs for different purposes, such as safety versus security and with different enforcement authorities, such as voluntary standards versus criminal penalties for non-compliance. Nevertheless, eight federal programs contain requirements or guidance that generally align with over half of the 18 CFATS program standards. Such similarities, as well as differences, indicate some overlap, duplication, and fragmentation among the nine programs, as well as potential security gaps depending on the program or programs under which a facility is regulated.

We have previously reported that fully addressing issues of overlap, duplication, and fragmentation is challenging, as they may involve long-standing programs with entrenched constituencies. The lack of comprehensive and reliable data on the number of federal programs,

such as on facilities regulated by multiple programs, compounds these challenges. The departments and agencies responsible for all nine of these chemical safety and security programs have previously worked together to enhance information collection and sharing in response to Executive Order 13650. The CFATS program, recognizing that its 18 standards overlap, has demonstrated a willingness to revisit its requirements to allow for flexibility, but additional steps could be taken amongst the nine programs to share information, identify, and reduce potentially duplicative information requirements. Additional steps could also be taken amongst those programs with fragmented requirements to better understand the extent to which security gaps may exist, and develop legislative proposals to address any security gaps.

Recommendations for Executive Action

We are making recommendations to each of the four agencies in our review to enhance information collection and sharing across agencies to support more informed decision-making, streamline reporting requirements, and reduce duplicative efforts related to their programs. Specifically:

The Secretary of DHS should direct its chemical safety and security programs to collaborate with partners and establish an iterative and ongoing process to identify the extent to which CFATS-regulated facilities are also covered by other programs with requirements or guidance that generally align with some CFATS standards. (Recommendation 1)

The Administrator of the EPA should direct its chemical safety and security programs to collaborate with partners and establish an iterative and ongoing process to identify the extent to which the facilities that it regulates are also covered by the CFATS program. (Recommendation 2)

The Director of ATF should direct its explosive materials programs to collaborate with chemical safety and security program partners and establish an iterative and ongoing process to identify the extent to which the facilities that it regulates are also covered by the CFATS program. (Recommendation 3)

The Secretary of Transportation should direct its hazardous materials transportation program to collaborate with chemical safety and security partners and establish an iterative and ongoing process to identify the extent to which the facilities that it regulates are also covered by the CFATS program. (Recommendation 4)

The Director of DHS's Cybersecurity and Infrastructure Security Agency should update CFATS program guidance or fact sheets to include a list of commonly accepted actions facilities may have taken and information they may have prepared pursuant to other federal programs, and disseminate this information. (Recommendation 5)

We are making a total of two recommendations to DHS and EPA to identify potential security gaps related to their programs. Specifically:

DHS's Cybersecurity and Infrastructure Security Agency should collaborate with the EPA to assess the extent to which potential security gaps exist at water and wastewater facilities and, if gaps exist, develop a legislative proposal for how best to address them and submit it to the Secretary of Homeland Security and Administrator of EPA, and Congress, as appropriate. (Recommendation 6)

The EPA should collaborate with the DHS's Cybersecurity and Infrastructure Security Agency to assess the extent to which potential security gaps exist at water and wastewater facilities and, if gaps exist, develop a legislative proposal for how best to address them and submit it to the Secretary of Homeland Security and Administrator of EPA, and Congress, as appropriate. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, ATF, DOT, and EPA. DHS, DOT, and EPA provided written comments which are reproduced in appendices III, IV, and V respectively. ATF did not provide written comments. For those departments that provided technical comments, we incorporated them as appropriate.

In its letter, DHS provided a general comment regarding our assessment of chemical programs' alignment with CFATS' risk-based performance standards. DHS acknowledged that as approximately 16 percent, or about 550, of the 3,300 facilities subject to CFATS regulations are also regulated by other federal departments and agencies, there may be some regulatory overlap and duplication. DHS also stated that, in the department's view, we overestimate the overlap in actual requirements imposed by CFATS and those of other programs when we assert that general alignment exists. In addition, DHS stated that we underestimate the reduction in potential impact of regulatory overlap alleviated by CFATS allowing facilities to use activities performed in response to other regulations for compliance with CFATS standards.

However, while we evaluated general alignment with the CFATS standards, we did not make a determination about the effectiveness of each program or the relative security of facilities regulated by each program. Notably, DHS does not periodically evaluate the extent to which its regulated facilities are regulated by other programs, which would allow it to identify the extent of overlap among such facilities and underscores the need for our first recommendation. Further, as stated in our report, general alignment does not mean that the requirements are the same. Rather, we considered general alignment to occur when actions required or authorized under other programs are similar to actions that facilities may take pursuant to the CFATS standards, to include in limited circumstances.

With regard to the seven recommendations in our report, agencies concurred with six and EPA did not concur with one:

We made four recommendations to each of the four agencies in our review to collaborate with chemical safety and security partners and establish an iterative and ongoing process to identify the extent to which CFATS-regulated facilities are also covered by other programs with requirements or guidance that generally align with some CFATS standards.

DHS concurred with recommendation 1, stating in its letter that reviewing the extent to which CFATS-regulated facilities are also covered by other programs will allow DHS and partner federal agencies to further reduce potential overlap and duplication, and better identify possible security gaps between regulatory regimes. DHS described planned steps to address the recommendation, such as collaborating with fellow federal agencies to identify facilities covered by multiple programs through the Chemical Government Coordinating Council, and anticipates addressing the recommendation by December 31, 2021. These actions, if fully implemented, should address the intent of this recommendation.

EPA concurred with recommendation 2, stating in its letter that both EPA and DHS will benefit from improved communication between the two agencies by ensuring its partnership with DHS is ongoing and iterative. EPA described planned steps to address the recommendation, including information sharing of facility data and EPA enforcement actions. EPA anticipates addressing the recommendation by December 31, 2021. These actions, if fully implemented, should address the intent of this recommendation.

ATF informed us via email that they had no comments on the draft report and neither agreed nor disagreed with recommendation 3. We will continue to monitor ATF's activities to assess whether this recommendation is implemented.

DOT concurred with recommendation 4, stating in its letter that DOT will provide a detailed response to the recommendation within 180 days of our final report's issuance. We will continue to monitor DOT's activities and response to this recommendation to assess whether the recommendation is implemented.

We made one recommendation (recommendation 5) to DHS's Cybersecurity and Infrastructure Security Agency to update CFATS program guidance or fact sheets to include a list of commonly accepted actions facilities may have taken and information they may have prepared pursuant to other federal programs, and disseminate this information.

DHS concurred with recommendation 5, stating in its letter that, among other actions, CISA will update or create a new guidance document or fact sheet by December 31, 2021, that includes a list of commonly accepted actions CFATS-regulated facilities may have taken and information they may have prepared pursuant to other federal programs and disseminate this information. This action, if fully implemented, should address the intent of this recommendation.

We made two recommendations (recommendations 6 and 7) to DHS and EPA to collaborate with each other to assess the extent to which potential security gaps exist at water and wastewater facilities and, if gaps exist, develop a legislative proposal for how best to address them and submit it to the Secretary of Homeland Security and the Administrator of EPA, and Congress, as appropriate.

DHS concurred with recommendation 6, stating in its comment letter that, among other actions, the department will work with EPA to identify and explore possible approaches for assessing potential security gaps that exist at water and wastewater facilities broadly. DHS anticipates that the security gap assessment will be completed by July 29, 2022. According to DHS's comment letter, DHS and the EPA will determine if any additional action is warranted. If it is determined that a significant security gap exists, DHS stated in its letter that it and EPA will identify and evaluate potential options for addressing that gap and acknowledged that one option of working with Congress to legislatively address the gap either through the removal of the existing water and wastewater facility

exemption from CFATS or by providing either DHS or EPA with new authority to regulate security at these facilities. DHS anticipates selecting an approach for addressing any security gaps by October 31, 2022. These actions, if fully implemented, should address the intent of this recommendation.

EPA did not concur with recommendation 7, stating in its comment letter that our report provides the detailed analysis that EPA and DHS can use as a starting point for discussion and that our recommendation to submit a legislative proposal is unnecessary and inappropriate because EPA and DHS have already provided testimony to Congress that a security gap exists and should be addressed. EPA also stated that a recommendation to develop a legislative proposal is inappropriate because the legislative branch develops legislation, not the executive branch. Finally, EPA stated that the agency agrees with our recommendation to collaborate across federal agencies to address potential security gaps and would concur with a recommendation to address gaps under current authorities.

We disagree with EPA's position. First, we did not identify the full range of security gaps that could exist at water and wastewater facilities. DHS and EPA are better positioned to conduct such an analysis given their more exhaustive data on potential vulnerabilities at such facilities. Second, executive branch agencies routinely submit legislative proposals for congressional consideration. While Congress exercises discretion on whether to act on such legislative proposals, executive branch agencies are often well-positioned to suggest specific approaches for solving concerns under their jurisdiction, such as security gaps. Third, as stated in our report, EPA and DHS senior officials have previously stated that there is a gap in the chemical security regulatory framework due to the exemption of drinking water and wastewater treatment facilities from CFATS. However, at the time of these statements, the two agencies had not conducted an assessment of possible security gaps that could be used to support such testimony and a proposed statutory change removing the exemption for such facilities.

For these reasons, we continue to believe that our recommendation is valid and that if DHS and EPA identify security gaps at water and wastewater facilities, developing a legislative proposal to address them may be appropriate. However, if DHS and EPA determine that they can adequately address identified security gaps under current authorities, taking action under such authorities would also satisfy our recommendation.

We are sending this report to interested congressional committees and the Acting Secretary of Homeland Security, the Administrator of the Environmental Protection Agency, the Director of ATF, and the Secretary of Transportation. 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 (206) 287-4804 or AndersonN@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 IV.

Nathan Anderson
Director
Homeland Security and Justice

List of Requesters

The Honorable Josh Hawley
United States Senate

The Honorable Ron Johnson
United States Senate

The Honorable James Lankford
United States Senate

The Honorable Gary C. Peters
United States Senate

The Honorable Kyrsten Sinema
United States Senate

Appendix I: Scope and Methodology

To address our first objective, to evaluate the extent to which overlap, duplication, and fragmentation may exist between the Chemical Facility Anti-Terrorism Standards (CFATS) program and other federal programs that regulate chemical safety and security, we reviewed executive orders related to chemical safety and security, statutes, programs' regulations, and other documents. Executive Order 13650–*Improving Chemical Facility Safety and Security* identified the Department of Homeland Security (DHS); the Environmental Protection Agency (EPA); and the Departments of Justice, Agriculture, Labor, and Transportation, and including representation from the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as agencies with regulatory authority in this area.[1] Specifically, we focused on: (1) DHS' CFATS program, (2) the U.S. Coast Guard's Maritime Transportation Security Act of 2002 (MTSA) program, (3) the Transportation Security Administration (TSA) rail security program, (4) TSA's pipeline security program, (5) ATF's explosive materials program, (6) EPA's Water Infrastructure Act program, (7) EPA's Risk Management Program, (8) EPA's Resource Conservation and Recovery Act (RCRA) program, and (9) the Department of Transportation (DOT) hazardous materials program.[2]

First, to analyze the extent to which these federal programs contain requirements or guidance that generally align with DHS's CFATS program standards, we compared these programs' requirements and guidance to the CFATS program's 18 risk-based performance standards

[1]Executive Order 13650–*Improving Chemical Facility Safety and Security* established a Chemical Facility Safety and Security working group, composed of representatives from DHS; EPA; and the Departments of Justice, Agriculture, Labor, and Transportation, and directed the working group to identify ways to improve coordination with state and local partners; enhance federal agency coordination and information sharing; identify opportunities to modernize policies, regulations and standards; and work with stakeholders to reduce chemical facility safety and security risks. See Exec. Order No. 13,650, 78 Fed. Reg. 48,029 (Aug. 7, 2013).

[2]We did not review all programs that address chemical safety and security, such as Department of Labor Occupational Safety and Health Administration requirements because they generally apply to labor issues beyond the scope of our review. The DOT also regulates the safety and security of liquefied natural gas transportation and storage under 49 C.F.R. part 193. Because the program focused on only one chemical common to the CFATS program—methane, we did not include this program in the scope of our review. We did not review Department of Energy or Department of Defense programs that apply to excluded facilities, which were beyond the scope of our review.

and associated guidance.[3] We determined that a program's requirements generally align with a CFATS standard when the relevant statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take to meet the CFATS standard, to include in limited circumstances. We considered program requirements and guidance to generally align with CFATS standards when actions required or authorized under the program have a different purpose or goal but may have the same effect as actions taken pursuant to the CFATS standard.

We supplemented our independent analyses with written responses from each program. Further, we interviewed officials from the nine programs to gain their perspectives on whether these programs have requirements or guidance that generally align with the CFATS program standards, as well as representatives from eight industry associations to gain additional understanding of which programs apply to certain types of facilities and on their perceptions of program alignment. We selected the eight industry associations because their membership includes facilities subject to the requirements and guidance of programs within the scope of our review and they are part of the Chemical Sector or Water and Wastewater Systems Coordinating Councils.[4] The information obtained from our

[3]Specifically, three analysts independently reviewed the programs' regulations, guidance, and other materials to determine if the programs contained requirements or guidance that generally aligned with each of the 18 CFATS standards. The three analysts compared their results and resolved any differences, and a senior attorney reviewed the unified assessment and supporting regulations, guidance, and other materials. For America's Water Infrastructure Act, we reviewed the statute, as there are no corresponding regulations. We also reviewed, among other documents, Coast Guard, *Navigation and Vessel Inspection Circular No. 03-03, change 2: Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 Clean Air Act Section 112(r)*, EPA 550-K-11-001 (Jan. 2011); and EPA, *General Guidance on Risk Management Programs for Chemical Accident Prevention* (40 CFR part 68), EPA 555-B-04-001 (March 2009).

[4]The specific methodology for selecting associations to meet with includes identifying associations, where possible or relevant, from the Chemical, Nuclear, Water and Wastewater Systems, and other Coordinating Councils established by DHS based on the 16 critical infrastructure sectors as defined by *Presidential Policy Directive/PPD- 21: Critical Infrastructure Security and Resilience*, released on February 12, 2013. These 16 critical infrastructure sectors have assets, systems, and networks, whether physical or virtual, that are considered so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Each sector has a self-organized and self-governed Coordinating Council that enables 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.

interviews is not generalizable, but provides insights into the programs that have regulations or guidance that align with CFATS.

Second, we evaluated the extent to which alignment with CFATS indicates overlap, duplication, and fragmentation and applied our framework for identifying such conditions.[5] We supplemented our analyses with written responses from each program, including asking each program whether it contained requirements or guidance for security measures beyond, in addition to, or more comprehensively than the CFATS standards. We developed counts of facilities subject to CFATS and the eight federal programs (e.g. ATF explosive materials program) that we determined contain regulations or guidance that generally align with some CFATS standards by obtaining the most recent available records and information from the respective responsible agencies, if available.[6] We obtained and analyzed these records on facilities subject to the ATF, EPA, and DOT programs in order to analyze and identify instances where the same facility was covered by both CFATS and another program (i.e., is subject to multiple programs) and indicate duplication or fragmentation with DHS' CFATS program. We selected CFATS as a comparison because (1) the CFATS program worked with some of the other programs to develop its standards and (2) DHS has designated the Cybersecurity and Infrastructure Security Agency (CISA), in which the CFATS program resides, as the lead component for government-wide critical infrastructure security and resilience.

To compare these data, we used statistical analysis software to identify facilities subject to CFATS and other programs by matching facility names from the eight programs with CFATS records, including addresses, and

[5]See GAO's Duplication and Cost Savings web page for links to the 2011 to 2019 annual reports: http://www.gao.gov/duplication/overview.

[6]For CFATS, we obtained and analyzed facility data, as of December 2019. For MTSA-regulated facilities, we obtained and analyzed Coast Guard facility data, as of December 2019. For TSA rail security, we obtained and analyzed inspection records related to rail shippers and receivers for fiscal years 2017, 2018, and 2019. For TSA pipeline security, we obtained and analyzed data for the top 100 critical pipeline system operators, as determined by TSA, as of February 2020. For ATF explosive materials, we obtained and analyzed licensee data, as of November 2019. For EPA's Risk Management Program, we obtained and analyzed EPA data, as of January 2020. For EPA's Resource Conservation and Recovery Act (RCRA) program, we obtained and analyzed data on Treatment, Storage, and Disposal facilities and large quantity generators of hazardous wastes, as of March 2020. For DOT hazardous materials program, we obtained and analyzed fiscal year 2019 data from the Hazardous Materials Registration System for facilities required to register.

combinations of names and addresses. To assess the reliability of the data, we reviewed documentation and information about the various systems used to house the data for these programs and spoke with or received information from knowledgeable officials about the processes for the collection and maintenance of the records and their quality assurance procedures. We also reviewed the data for missing data or obvious errors, and interviewed managers of the various data systems. While the information in the data sets provided by each program was sufficiently reliable for the purposes of documenting the number of facilities subject to the programs and for our analyses, issues with the comparability of information in each data set exist, which we discuss in this report.[7]

We also interviewed officials from the nine programs to gain their perspectives on program alignment, as well as representatives from the eight industry associations mentioned above to obtain their perspectives on the effect of alignment and nonalignment on their members. Finally, we interviewed a nongeneralizable sample of six facility owners and operators, selected based on their being subject to CFATS and ATF programs, to obtain their perspectives on the impact of compliance with these programs and similarities and differences among them that indicate overlap, duplication, and fragmentation.[8]

To address our second objective, because we identified nine federal programs that contain requirements or guidance that indicate some overlap, duplication, and fragmentation, we analyzed the extent to which the CFATS program—co-chair of the Chemical Facility Safety and Security Working Group (working group)—coordinated with the other

[7]We used statistical analysis software to match facility names, addresses, and combinations to identify the number of facilities subject to CFATS and the other programs, and due to the limitations discussed later in this report we were able to identify some facility matches, which we identify as a minimum threshold, but there may be more.

[8]We conducted interviews on the phone because of impacts to government operations related to Coronavirus Disease (COVID-19). While we interviewed six owners and operators where CFATS program standards and ATF requirements apply, we were not able to interview facility owners and operators subject to other programs including MTSA, Risk Management Program, and TSA rail and pipeline programs. We identified potential facilities to interview based on the results of our analysis of CFATS and ATF facility records, and worked with an association to obtain contact information for the facilities.

eight programs.[9] Specifically, we identified a May 2014 report co-authored by DHS that identified federal actions to enhance federal agency coordination and information sharing.[10] We verified with officials from CFATS and other programs within our scope that this report and related documents were intended to achieve improved coordination, and obtained an updated interagency collaborative agreement signed in late 2018.[11] We assessed these reports, data, documents, and subsequent CFATS program actions against specific Executive Order 13650– *Improving Chemical Facility Safety and Security* provisions. For example, the order directed the working group to develop a plan to support and further enable efforts by state and local governments and chemical facility owners and operators to improve chemical facility safety and security that, among other things: (1) identifies ways to ensure that state and local chemical safety and security partners have access to key information in a useable format; and (2) identifies areas where joint collaborative programs can be developed or enhanced, including by better integrating existing authorities, jurisdictional responsibilities, and regulatory programs in order to achieve a more comprehensive engagement on chemical risk management. The executive order also directs the working group to produce a proposal for a coordinated, flexible data-sharing process that can be utilized to track data submitted to agencies for federally-regulated chemical facilities and to identify and recommend possible changes to

[9]Executive Order 13650–*Improving Chemical Facility Safety and Security* established a Chemical Facility Safety and Security working group, composed of representatives from DHS; EPA; and the Departments of Justice, Agriculture, Labor, and Transportation, and directed the working group to take actions to improve coordination with state and local partners; enhance federal agency coordination and information sharing; identify opportunities to modernize policies, regulations and standards; and work with stakeholders to identify and share best practices. See Exec. Order No. 13,650, 78 Fed. Reg. 48,029 (Aug. 7, 2013).

[10]*Actions to Improve Chemical Facility Safety and Security—A Shared Commitment*, Report for the President (May 2014). See Exec. Order No. 13650, 78 Fed. Reg. at 48,029, § 2(c) (directing the submission of a status report within 270 days of the date of the Executive Order).

[11]Because actions intended to achieve improved coordination may require actions to be taken by multiple agencies, while the focus of our review was on the CFATS program, we note throughout that some actions may be necessary by partner agencies in order for the CFATS program to improve collecting and sharing information.

streamline and otherwise improve data collection to meet the needs of the public and federal, state, local, and tribal agencies.[12]

We analyzed comments to the CFATS proposed rule and DHS responses to identify the history of the program, including whether the CFATS program addressed concerns during the rulemaking process about potential duplication.[13] We analyzed CFATS records of facilities subject to its program requirements, selected based on instances where the facilities detailed information prepared for other programs as part of their security plans for CFATS, the results of which are not generalizable but provide examples of the potential for reusing information from various programs as part of CFATS security plans. We analyzed all 21 CFATS fact sheets, and other CFATS program guidance covering such topics as compliance inspections and chemicals of interest to identify program guidance on reusing information among programs that address chemical safety and security.

We analyzed interagency agreements between the CFATS program and other chemical safety and security programs, including 10 regional agreements on field operations coordination and information sharing among chemical safety and security programs. In addition, we compared DHS and working group actions with the DHS *National Infrastructure Protection Plan*,[14] which establishes a framework for critical infrastructure partners, including federal agencies, to understand how critical infrastructure protection, such as chemical security, is being conducted, and to identify duplicative efforts and gaps across jurisdictions.

[12]Executive Order 13650–*Improving Chemical Facility Safety and Security* further directs the working group to deploy a pilot program to validate best practices and to test innovative methods for federal interagency collaboration regarding chemical facility safety and security. In 2018, working group leaders reaffirmed their agencies commitment to the working group activities established pursuant to the Executive Order 13650, in a signed charter that described continued commitment among relevant agencies to coordinate information sharing and review policies and regulations associated with chemical safety and security to minimize conflicts and overlap, among other things.

[13]See 72 Fed. Reg. 17,687 (Apr. 9, 2007).

[14]DHS, *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013). PPD-21 and the NIPP also call for other federal departments and agencies to play a key role in CI security and resilience activities. Presidential Policy Directive/PPD-21 revoked HSPD-7 and realigns the 18 sectors into 16 critical infrastructure sectors, and provides that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

The information and communication component of internal control was significant to this objective, along with the underlying principles that management identifies, obtains from relevant internal and external sources, and uses quality information in an iterative and ongoing process, to internally and externally communicate the necessity of quality information. We assessed the agencies' policies and procedures for controlling relevant information from internal and external sources and using such information to make informed decisions. Specifically, we compared DHS and working group partner actions against our *Standards for Internal Control for the Federal Government*, which emphasizes the importance of quality information for management to make informed decisions, including the use of relevant data from reliable sources collected through an iterative and ongoing process.[15]

Finally, Executive Order 13650 directed the working group to take actions focused on, among other things, (1) identifying opportunities to modernize policies, regulations, and standards; (2) improving coordination; (3) enhancing information collection and sharing; and (4) reducing chemical safety and security risks—such as by identifying and closing security gaps.[16] We evaluated actions taken in response to Executive Order 13650, which were detailed in a 2014 report jointly issued by DHS partner agencies, and subsequent CFATS program and partner agency standard operating procedures and actions to enhance federal agency coordination and information sharing as of June 2020.

In addition, we conducted structured interviews with officials from each of the nine programs on the extent and effectiveness of coordination with CFATS. We interviewed program officials from CFATS, TSA, MTSA, America's Water Infrastructure Act, RCRA, Risk Management Program, ATF, and DOT to obtain their perspectives on the current status of collaboration, current operating procedures and challenges, if any, and to

[15]*Standards for Internal Control in the Federal Government* directs managers to use quality information to achieve program objectives, where "quality" means, among other characteristics, current, complete, and accurate. GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014) In addition, DHS's Information Quality Guidelines state that all DHS component agencies should treat information quality as integral to every step of the development of information, including creation, collection, maintenance, and dissemination. The DHS guidelines also state that agencies should substantiate the quality of the information disseminated through documentation or other appropriate means. Department of Homeland Security, Information Quality Guidelines, (Washington, D.C.: Mar. 2011).

[16]We focused on these goals because they involve federal collaboration and generally align with the information and communication component of internal control.

assess the extent to which CFATS and partners' actions align with Executive Order 13650 and related working group actions.

We conducted this performance audit from February 2020 to January 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Alignment of Eight Regulatory Programs with the Chemical Facility Anti-Terrorism Standards

The Department of Homeland Security (DHS) established its Chemical Facility Anti-Terrorism Standards (CFATS) program to assess the risks posed by chemical facilities and classify those designated as high-risk, among other things. High-risk facilities must implement security measures that meet the CFATS program's 18 risk-based performance standards.[1] This appendix summarizes the extent of general alignment between the CFATS program's 18 risk-based performance standards and requirements and guidance of eight programs that could address chemical security. Programs include the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) explosive materials program, Transportation Security Administration (TSA) rail security requirements program, TSA pipeline security guidelines program, U.S. Coast Guard's (Coast Guard) Maritime Transportation Security Act of 2002 (MTSA) program, Department of Transportation (DOT) hazardous materials transportation requirements program, Environmental Protection Agency's (EPA) Resource Conservation and Recovery Act (RCRA) hazardous waste program, EPA's Water Infrastructure Act program, and EPA's Risk Management Program. We determined that a program's requirements generally align with a CFATS standard when the relevant statutes, regulations, guidance, and other materials require or authorize actions that are similar to actions that facilities may take to meet the CFATS standard, to include in limited circumstances.[2] We considered program requirements and guidance to generally align with a CFATS standard when actions required or authorized under the program have a different purpose or goal but may have the same effect as actions taken pursuant to the CFATS standard.

[1]The 18 risk-based performance standards identify areas for which a facility's security posture are to be examined, such as perimeter security, access control, and cybersecurity. 6 C.F.R. § 27.230

[2]Specifically, three analysts independently reviewed the programs' regulations, guidance, and other materials to determine if the programs contained requirements or guidance that generally aligned with each of the 18 CFATS standards. The three analysts compared their results and resolved any differences, and a senior attorney reviewed the unified assessment and supporting regulations, guidance, and other materials. For America's Water Infrastructure Act, we reviewed the statute, as there are no corresponding regulations. We also reviewed, among other documents, Coast Guard, *Navigation and Vessel Inspection Circular No. 03-03, change 2: Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 Clean Air Act Section 112(r)*, EPA 550-K-11-001 (Jan. 2011); and EPA, *General Guidance on Risk Management Programs for Chemical Accident Prevention* (40 CFR part 68), EPA 555-B-04-001 (March 2009).

ATF explosive materials program. Approximately 10,000 licensees and permittees who manufacture, import, sell, or store any explosive materials are subject to ATF requirements and guidance intended to ensure the safe and secure storage of explosive materials. ATF regulations focus on the storage of explosives and not overall facility/site security, and compliance can be achieved by meeting material storage, recordkeeping, and conduct of business requirements, among other things.[3] In addition to ATF requirements, ATF publishes newsletters, rulings, open letters, and other documents to help the explosives industry understand their obligations under the federal explosives statutes and regulations. For example, ATF has published guidance on recordkeeping, storage requirements, fireworks safety and security, disaster preparedness, and heightened security letters, among others. ATF conducts two types of inspections at facilities subject to its regulations. During its initial inspection, ATF inspectors review all applicable explosives statutes and regulations with the license or permit applicant, and evaluate the applicant's proposed procedures for complying with ATF program requirements. During an explosives compliance inspection, ATF inspectors are to review the explosive material acquisition and disposition records to ensure that transfers of explosive materials were lawful, inventory and other records, and ensure that explosive materials are stored in accordance with ATF regulations, among other things. We found that ATF programs for explosive materials contain requirements and guidance that generally align with 11 of the 18 CFATS standards (see table 4. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

[3]See 27 C.F.R. pt. 555, subpt. K.

Table 4: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Explosive Materials Program Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	ATF	Examples of program requirements and guidance
Restrict area perimeter	X	X	• Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. • ATF does not require licensees or permittees to establish an area perimeter with restricted access, although it does require that all explosive materials be kept in locked structures meeting ATF-specified criteria. However, in rare circumstances, ATF has approved an alternate method or procedure in which a permittee or licensee employs area perimeter security measures to provide a substantially equivalent level of security to ATF requirements. For example, in response to inquiries from members of the explosives industry concerning the preloading and temporary storage of blasting agents on bulk delivery vehicles, ATF ruled that it would approve alternative methods or procedures when specified criteria are met, including the establishment of outer perimeter security, which may be met through means such as a locked gate, security guards, fencing, natural features, or a combination of these.[a]
Secure site assets	X	X	• The CFATS program requires facilities to secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion detection systems. • In general, ATF requires that its licensees and permittees secure all explosive materials in locked structures meeting ATF-specified criteria, and it must verify by inspection that applicants for user permits and licenses have places of storage for explosive materials that satisfy the standards of safety and security set forth in regulation. According to ATF guidance, the purpose of an explosives inspection is to, among other things, identify areas of weakness and vulnerability in security and internal controls in order to prevent prohibited persons and terrorists from obtaining explosive materials
Screen and control access	X	X	• Under CFATS, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. • ATF does not require or direct licensees and permittees to screen and control access to their facilities, but its regulations provide, in general, that ATF will conduct a background check of responsible persons and employees who will be authorized by the employer to possess explosive materials in the course of employment with the employer, and that all explosive materials must be kept in locked structures meeting ATF-specified criteria, using locks that meet requisite standards.[a]
Deter, detect, and delay	X	X	• Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. • ATF requires that licensees and permittees store and maintain explosive materials using structures, and locks for securing them, that meet ATF-specified criteria and standards.[a]

CFATS risk-based performance standard	CFATS	ATF	Examples of program requirements and guidance
Shipping, receipt, and storage	X	X	• Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of quantity and physical location of hazmat. • ATF requires, in general, that only a licensee or permittee knowingly may transport, ship, cause to be transported, or receive any explosive materials. Among other things, ATF guidance provides that inspectors should verify proper receipt and disposition entries in required records and review the licensee's internal controls to determine whether transactions are properly reflected in required records.
Theft and diversion	X	X	• Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. • ATF requires, among other things, that licensees and permittees store and maintain explosive materials using structures, and locks for securing them, that meet ATF-specified criteria and standards. ATF conducts compliance inspections to determine if a licensee or permittee is complying with federal laws and regulations and to detect and prevent the diversion of explosive materials from legal to illegal commerce, including identifying areas of weakness and vulnerability in security and internal controls in order to prevent prohibited persons and terrorists from obtaining explosives materials.
Sabotage	X	X	• Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. • ATF encourages all licensees and permittees to follow best practices, such as inspecting perimeter security and reporting any indications of attempted theft (e.g., cut fences or unlocked gates), visually inspecting magazines and locks for any damage affecting their theft-resistance, and reporting any suspicious behavior at or near explosives storage and distribution areas. ATF regulations provide, in general and among other things, that ATF will conduct background checks on individuals authorized by an employer to possess explosive materials, and establish requirements for storing and securing explosives.[a]
Cyber	X	—	• Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. • ATF regulations and guidance do not include a cybersecurity program element.
Response	X	—	• Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders. • ATF regulations and guidance do not include a program element to develop and exercise an emergency plan to respond to security incidents.

CFATS risk-based performance standard	CFATS	ATF	Examples of program requirements and guidance
Monitoring	X	—	• Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. • ATF regulations and guidance do not include a program element to maintain such monitoring, communications, and warning systems.
Training	X	—	• Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. • ATF regulations and guidance do not include a security training, exercises, and drills program element.
Employee background checks	X	X	• Under the CFATS program, facilities must perform appropriate background checks for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. • ATF conducts background checks on permittees, licensees, applicants, responsible persons, and employees who possess explosives either in interstate or intrastate commerce. ATF regulations provide that ATF will conduct background checks on individuals who will be authorized by an employer to possess explosive materials.
Elevated threats	X	—	• Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. • ATF regulations and guidance do not address escalating the level of protective measures for periods of elevated threats as a program element.
Specific threats, vulnerabilities, or risks	X	—	• Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment by, among other things, using new information and increasing security measures. • ATF regulations and guidance do not include a program element that requires licensees or permittees to address specific threats, vulnerabilities, or risks that are new or may not have been previously identified.
Reporting of significant security incidents	X	X	• Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. • ATF requires licensees and permittees to document daily inventory and report any theft or loss to ATF within 24 hours of discovery, as well as to appropriate local authorities.

CFATS risk-based performance standard	CFATS	ATF	Examples of program requirements and guidance
Significant security incidents and suspicious activities	X	X	• Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this standard. • ATF requires permittees and licensees to report any theft or loss to ATF within 24 hours of discovery, as well as to appropriate local authorities. According to ATF guidance, inspectors may recommend or advise a licensee or permittee to report any suspicious activity to ATF.
Officials and organization	X	—	• Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. • ATF regulations and guidance do not include a program element for licensees and permittees to identify officials or organizations responsible for security and for compliance.
Records	X	X	• Under the CFATS program, facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request. • ATF requires licensees and permittees to keep records in permanent form and in a manner consistent with ATF requirements on premises for, in general, five years from the date of a transaction. Among other things, licensees and permittees must record a daily summary of the inventory of explosive materials on hand and, not later than the close of the next business day, shall record by manufacturer's name or brand name, the total quantity received in and removed during the day, and the total remaining on hand at the end of the day.

Source: GAO analysis of CFATS and ATF regulations and guidance. | GAO-21-12

[a]ATF's jurisdiction generally does not extend to the entire facility within which explosive materials are stored. However, ATF's program accounts for measures that, within the context of ATF's jurisdiction and based on our analysis, generally address the CFATS standard such that we consider ATF's program to be in general alignment with this CFATS standard.

TSA's rail security program. The TSA rail security program regulates freight railroad carriers and rail operations at certain, fixed-site facilities that ship or receive (within high threat urban areas) specified hazardous materials by rail.[4] The hazardous materials subject to this regulation include certain explosives, toxic inhalation hazardous materials, and radioactive materials and collectively are known as rail security-sensitive

[4]High Threat Urban Areas (HTUA) are defined as "an area comprising one or more cities and surrounding areas including a 10-mile buffer zone." See 49 C.F.R. § 1580.3; 49 C.F.R. pt. 1580 app. A.

materials.[5] The program requires certain freight rail shippers and receivers within high-threat urban areas to designate a rail security coordinator, notify TSA regarding any significant security concerns, and ensure a secure chain of custody of rail cars containing the hazardous materials, and be able to provide location and shipping information for certain rail cars, among other things.[6] The program adopts a risk-based approach by focusing on shipments of rail security-sensitive materials to reduce rail car security vulnerabilities. We found that the TSA rail security program contains requirements that generally align with over half of the CFATS standards—11 of 18 (see table 5. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

TSA's Pipeline Security program. TSA's Pipeline Security Program is designed to enhance the security preparedness of the nation's hazardous liquid and natural gas pipeline systems.[7] Pursuant to its authority, TSA's Pipeline Security Branch first issued its voluntary *Pipeline Security Guidelines* in 2011, and released revised guidelines in March 2018.[8] The

[5]Toxic Inhalation Hazardous materials include chlorine (used in water treatment) and anhydrous ammonia (used in agriculture). In addition, shipments of these materials, especially chlorine, frequently move through densely populated areas to reach, for example, water treatment facilities that use these products. If released from a railcar in large quantities under certain atmospheric conditions, these materials could result in fatalities to the surrounding population. Specifically, rail security-sensitive materials are: (1) a rail car containing more than 2,268 kg (5,000 lbs) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 C.F.R. § 173.50; (2) a tank car containing a material poisonous by inhalation as defined in 49 C.F.R. § 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 C.F.R. § 173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 C.F.R. § 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 C.F.R. § 173.133(a), excluding residue quantities of these materials; and (3) A rail car containing a highway route-controlled quantity of a Class 7 (radioactive) material, as defined in 49 C.F.R. § 173.403. 49 C.F.R. § 1580.100.

[6]49 C.F.R. pt. 1580, subpt. B.

[7]The Unites States has over 200,000 miles of hazardous liquid pipeline that transport crude oil, diesel fuel, gasoline, jet fuel, anhydrous ammonia, and carbon dioxide.

[8]See Transportation Security Administration, *Pipeline Security Guidelines* (March 2018). The Implementing Recommendations of the 9/11 Commission Act of 2007 directs the Secretary of Homeland Security, in conjunction with the Secretary of Transportation, to develop and transmit to pipeline operators security recommendations for natural gas and hazardous liquid pipelines and pipeline facilities and, if deemed appropriate, to promulgate regulations and carry out necessary inspection and enforcement actions. See Pub. L. No. 110-53, § 1557(d), 121 Stat. 266, 475-76 (codified at 6 U.S.C. § 1207(d)). TSA has not issued regulations for the pipeline sector under this authority but instead relies on voluntary compliance with the agency's security guidelines and best practice recommendations.

guidelines include TSA's recommendations for pipeline industry security practices, such as establishing a corporate security program, conducting security vulnerability assessments, and identifying critical facilities.[9] The guidelines also recommend facility security and cybersecurity measures. In response to the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA identifies the top 100 critical pipeline system operators in the nation.[10] To do so, it uses various risk factors and system annual throughput, which is based on the amount of hazardous liquid or natural gas product transported through a pipeline in 1 year. Additionally, TSA's Pipeline Security Branch is responsible for conducting voluntary Corporate Security Reviews and Critical Facility Security Reviews, which assess the extent to which the 100 most critical pipeline operators are following the intent of TSA's Pipeline Security Guidelines.[11] According to TSA officials, TSA oversees a facility where the pipeline begins all the way through the transmission to the end user. The supply chain of the pipeline (e.g., valves, metering stations, and other components within the pipeline necessary to transport the product around the nation) is where TSA provides oversight. We found that the Pipeline Security Program contains guidelines that generally align with 17 of 18 CFATS standards (see table 5. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

[9]We reported on pipeline security in December 2018. Among other things, we recommended TSA implement a documented process for reviewing, and if necessary, for revising TSA's Pipeline Security Guidelines at regular defined intervals and define key terms within its criteria for determining critical facilities. As of October 1, 2020, TSA has completed action on six of the 10 GAO recommendation. See GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: Dec. 18, 2018).

[10]See 6 U.S.C. § 1207(b). According to TSA Pipeline Security program officials, even though there are over 3,000 pipeline operators in the U.S., the top 100 critical pipeline system operators in the country represent approximately 85 percent of the energy throughput in the nation.

[11]Corporate Security Reviews are voluntary reviews of a pipeline owner's corporate policies and procedures. Critical Facility Security Reviews are voluntary onsite reviews of critical pipeline facilities, as well as other selected pipeline facilities throughout the nation. TSA requests selected operators to participate in these reviews, but operators can decline to participate. However, according to TSA program officials, no operator has declined to participate in one of these reviews.

Table 5: Transportation Security Administration (TSA) Rail and Pipeline Security Programs Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Restrict area perimeter	X	X	X	• Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. • Under TSA Pipeline Security program, facilities should employ measures to impede unauthorized access to facilities, maintain fences, if used, without gaps around gates or underneath the fence line, and ensure that there is a clear zone for several feet on either side of the fence. Critical facilities should create a security perimeter that impedes unauthorized vehicles from entering the facility perimeter or critical areas by installing and maintaining barriers and install gates of an equivalent quality to the barrier to which they are attached. • Under the TSA Rail Security program, facilities must keep rail security-sensitive materials rail cars in a rail secure area until it is shipped (for shippers) or unloaded (for receivers). The facilities must use physical security measures to ensure no unauthorized persons gain access to the rail secure area and may select lighting, video surveillance, or other appropriate methods besides fencing to meet the performance standard. For example, facilities may select technology such as intelligent video, passive intrusion detection, perimeter alarms, or advanced video surveillance systems.
Secure site assets	X	X	X	• Under the CFATS program, facilities must secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion-detection systems. • Under TSA Pipeline Security program guidelines, facilities should employ measures to impede unauthorized access to facilities and restricted areas within facilities. Critical facilities should create a security perimeter that impedes unauthorized vehicles from entering the facility perimeter or critical areas by installing and maintaining barriers and provide critical areas with security measures to monitor and assess unauthorized access 24 hours a day, 7 days a week. • Under the TSA Rail Security program, facilities must keep rail security-sensitive materials rail cars in a rail secure area until it is shipped (for shippers) or unloaded (for receivers). The facilities must use physical security measures to ensure no unauthorized persons gain access to the rail secure area and may select lighting, video surveillance, or other appropriate methods besides fencing to meet the performance standard.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Screen and control access	X	X	X	• Under the CFATS program, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. • Under TSA Pipeline Security program guidelines, facilities should employ measures to impede unauthorized persons from gaining access to the facility and restricted areas within a facility and develop identification and badging procedures for personnel who have access to secure areas or sensitive information. Critical facilities should monitor and escort visitors and ensure that company or vendor identification is visibly displayed by personnel while on-site. • Under the TSA Rail Security program, facilities must keep rail security-sensitive materials rail cars in a rail secure area until it is shipped (for shippers) or unloaded (for receivers). The facilities must use physical security measures needed to ensure no unauthorized persons gain access to the rail secure area and may select lighting, video surveillance, or other appropriate methods besides fencing to meet the performance standard.
Deter, detect, and delay	X	X	X	• Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. • Under TSA Pipeline Security program guidelines, facilities should employ measures to impede unauthorized persons from gaining access to the facility and restricted areas within the facility. Critical facilities should provide sufficient illumination for human or technological recognition of intrusion into the facility perimeter or critical areas. In addition, critical facilities should provide critical areas with security measures to monitor and assess unauthorized access 24 hours a day, 7 days a week. • Under the TSA Rail Security program, shippers must physically inspect rail cars before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; and suspicious items or items that do not belong, including the presence of an improvised explosive device. Shippers must also keep the rail car in a rail secure area from the time the security inspection mentioned above until the freight railroad carrier takes physical custody of the rail car. Receivers must ensure that the receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car and keep the rail car in a rail secure area until the car is unloaded.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Shipping, receipt, and storage	X	—	X	• Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of the quantity and physical location of hazmat. • TSA Pipeline Security program regulations and guidance do not address shipping, receipt, and storage. • Under the TSA Rail Security program, facilities are to have procedures in place to determine the location and shipping information of rail cars within their physical custody or control that contain rail security-sensitive materials and, upon request by TSA, be able to report the location and shipping information to TSA within 5 or 30 minutes, depending on the number of rail cars and type of carrier. Shippers must also physically inspect rail cars before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; and suspicious items or items that do not belong, including the presence of an improvised explosive device. Additionally, shippers must keep the rail car in a rail secure area from the time the security inspection mentioned above until the freight railroad carrier takes physical custody of the rail car and document the transfer of custody to the railroad carrier in writing or electronically. Receivers must ensure that the receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car, keep the rail car in a rail secure area until the car is unloaded, and document the transfer of custody from the carrier in writing or electronically.
Theft and diversion	X	X	X	• Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. • Under TSA Pipeline Security program guidelines, facilities should employ measures to impede unauthorized persons from gaining access to the facility and restricted areas and develop identification and badging procedures for personnel who have access to secure areas and sensitive information. Critical facilities should monitor and escort visitors at critical facilities and ensure that company or vendor identification is visibly displayed by personnel while on-site. • Under the TSA Rail Security program, shippers must physically inspect rail cars before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; and suspicious items or items that do not belong, including the presence of an improvised explosive device. Additionally, shippers must keep the rail car in a rail secure area from the time the security inspection mentioned above until the freight railroad carrier takes physical custody of the rail car and document the transfer of custody to the railroad carrier in writing or electronically. Receivers must ensure that the receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car, keep the rail car in a rail secure area until the car is unloaded, and document the transfer of custody from the carrier in writing or electronically.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Sabotage	X	X	X	• Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. • Under TSA Pipeline Security program guidelines, facilities should employ measures to impede unauthorized persons from gaining access to the facility and restricted areas, develop identification and badging policies for personnel who have access to secure areas or sensitive information, and establish policies for applicant pre-employment screening and behavioral criteria for disqualification of applicants and employees. Critical facilities should monitor and escort visitors at critical facilities and ensure that company or vendor identification is visibly displayed by personnel while on-site. • Under the TSA Rail Security program, shippers must physically inspect rail cars before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; and suspicious items or items that do not belong, including the presence of an improvised explosive device. Additionally, shippers must keep the rail car in a rail secure area from the time the security inspection mentioned above until the freight railroad carrier takes physical custody of the rail car and document the transfer of custody to the railroad carrier in writing or electronically. Receivers must ensure that the receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car, keep the rail car in a rail secure area until the car is unloaded, and document the transfer of custody from the carrier in writing or electronically.
Cyber	X	X	—	• Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. • Under TSA Pipeline Security program guidelines, facilities should consider the approach outlined in the NIST Framework. In addition, facilities should implement cybersecurity measures outlined in the guidelines, to include developing comprehensive network diagrams, establishing unique accounts for every user, and implementing processes to generate alerts and log cybersecurity events in response to anomalous activity. • TSA Rail Security program regulations and guidance do not address cybersecurity.
Response	X	X		• Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders. • Under TSA Pipeline Security program guidelines, facilities should implement procedures for responding to security incidents or emergencies and conduct periodic security drills or exercises, to include announced or unannounced tests of security and incident plans. Critical facilities should also conduct outreach to nearby law enforcement agencies to ensure awareness of the facility's functions and significance. • TSA Rail Security program regulations and guidance do not address response planning.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Monitoring	X	X	—	• Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. • Under TSA Pipeline Security program guidelines, facilities should develop and implement a maintenance program to ensure security systems are in good working order, and identify and respond to security equipment malfunctions or failures in a timely manner. Critical facilities should also provide an equivalent level of protective security measures to mitigate risk during power outages, security equipment failure, or extended repair of security systems. • TSA Rail Security program regulations and guidance do not address monitoring.
Training	X	X	—	• Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. • Under TSA Pipeline Security program guidelines, facilities should provide security awareness briefings, to include security incident recognition and reporting procedures, for personnel with unescorted access upon hiring and every three years thereafter. Critical facilities should provide security training to personnel assigned security duties upon hiring and annually thereafter. In addition, facilities should conduct periodic security drills or exercises, to include announced or unannounced tests of security and incident plans. • TSA Rail Security program regulations and guidance do not address security training at rail facilities.
Employee background checks	X	X	—	• Under the CFATS program, facilities must perform appropriate background checks for facility personnel and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. • Under TSA Pipeline Security program guidelines, facilities should develop identification and badging for personnel, and establish policies and procedures for applicant pre-employment screening and behavioral criteria for disqualification of applicants and employees. Critical facilities should conduct pre-employment background investigations of applicants for positions that are authorized regular unescorted access to sensitive areas, among other things. Investigations should verify identity, check criminal history, and validate legal authorization to work. • TSA Rail Security program regulations and guidance do not address employee background checks.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Elevated threats	X	X	—	• Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. • Under TSA Pipeline Security program guidelines, facilities should implement procedures for responding to pertinent National Terrorism Advisory System (NTAS) Bulletins or Alerts. Critical facilities should follow TSA's recommended security measures during periods of heightened threat, as disseminated by NTAS alerts. For example, if an Elevated or Imminent alert is disseminated by NTAS, facilities should implement the protective measures described in the tables provided by DHS. • TSA Rail Security program regulations and guidance do not address escalating the level of protective measures for periods of elevated threats.
Specific threats, vulnerabilities, or risks	X	X	—	• Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment, by, among other things, using new information and increasing security measures. • Under TSA Pipeline Security program guidelines, facilities should conduct security vulnerability assessments on a periodic basis, not to exceed 36 months, and within 12 months after completion of a significant enhancement or modification to the facility. Also, if an Elevated or Imminent alert is disseminated by NTAS, critical facilities should implement the protective measures described in the tables provided by DHS. • TSA Rail Security program regulations and guidance do not address specific threats, vulnerabilities, or risks that are new or may not have been previously identified.
Reporting of significant security incidents	X	X	X	• Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. • Under TSA Pipeline Security program guidelines, facilities should develop internal and external notification requirements and procedures for security events and document and periodically update contact information for Federal, state, and local homeland security and law enforcement agencies. Critical facilities should ensure primary and alternate communication capabilities exist for internal and external reporting of appropriate security events and information. Facilities should also report actual or suspected cyber-attacks to the National Cybersecurity and Communications Integration Center. • Under the TSA Rail Security program, facilities are to immediately report potential threats and significant security concerns to DHS's Freedom Center. Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to interference with the train crew, bomb threats, reports or discovery of suspicious items that result in the disruption of railroad operations, and indications of tampering with rail cars.

CFATS risk-based performance standard	CFATS	TSA Pipeline	TSA Rail	Examples of program requirements and guidance
Significant security incidents and suspicious activities	X	X	X	• Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this CFATS standard. • Under TSA Pipeline Security program guidelines, facilities should develop internal and external notification requirements and procedures for security events, and critical facilities should establish a defined process for receiving, handling, disseminating, and storing security and threat information. Facilities should also define the types of events that constitute a breach of security, describe the procedures for investigating security incidents, and develop recordkeeping policies for security information. • Under the TSA Rail Security program, facilities are to immediately report potential threats and significant security concerns to DHS's Freedom Center. Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to interference with the train crew, bomb threats, reports or discovery of suspicious items that result in the disruption of railroad operations, and indications of tampering with rail cars.
Officials and organization	X	X	X	• Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. • Under TSA Pipeline Security program guidelines, facilities should identify the primary and alternate security manager or officer responsible for executing and maintaining the security plan. Further, facilities should describe the responsibilities and duties of personnel assigned to security functions. • Under the TSA Rail Security program, facilities are to designate a Rail Security Coordinator, who will serve as the liaison to TSA for intelligence information, security-related activities and ongoing communications with TSA. The Rail Security Coordinator must be available 24 hours per day, and coordinate security practices and procedures with appropriate law enforcement and emergency response agencies.
Records	X	X	X	• Under CFATS, facilities must create, maintain, protect, store, and make available for inspection by DHS certain records related to its security program. • Under TSA Pipeline Security program guidelines, facilities should develop and document recordkeeping policies and procedures for security information, and make security information records available to TSA upon request. For example, facilities should retain documents such as the Corporate Security Plan, criticality assessments, training records, security drill reports, and incident response plans. • Under the TSA Rail Security program, facilities are to document the transfer of custody to and from the railroad carrier in writing or electronically, maintain them for at least 60 calendar days, and make them available to TSA upon request.

Source: GAO analysis of CFATS and TSA regulations and guidance. | GAO-21-12

MTSA program. MTSA requires facility security plans to deter a transportation security incident, which can include protecting the nation's waterfront facilities from terrorist attacks. As a result, security of

chemicals transported at or on U.S. waterways is only one aspect of the facility plans required by the MTSA program. Owners or operators of facilities subject to MTSA regulations are required to, among other things, designate a facility security officer, ensure that a facility security risk assessment was conducted, and ensure that a facility security plan is approved and implemented for facilities (such as factories, cargo terminals, and power plants).[12] The basic aim of such plans is to develop measures to mitigate potential vulnerabilities that could otherwise be exploited to kill people, cause environmental damage, or disrupt transportation systems and the economy. Based on our assessment of the CFATS and MTSA programs' regulations and guidance we found that the two programs' security measures generally align. Specifically, the MTSA program contains requirements or guidance that generally align with all 18 of the CFATS risk-based performance standards that facilities regulated as high-risk under the CFATS program are generally required to address (see table 6. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

Table 6: Maritime Transportation Security Act (MTSA) Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	MTSA	Examples of program requirements and guidance
Restrict area perimeter	X	X	Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. Under the MTSA program, the facility must have the capability to continuously monitor—through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment—the facility and its approaches, on both land and water, and restricted areas within the facility.
Secure site assets	X	X	The CFATS program requires facilities to secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion detection systems. Under the MTSA program, facilities are to have procedures to secure dangerous substances and devices that are authorized to be on the facility. Facilities are also to designate restricted areas in order to protect sensitive security areas, and security and surveillance equipment, among other things.

[12]33 C.F.R. pt. 105, subpt. B.

CFATS risk-based performance standard	CFATS	MTSA	Examples of program requirements and guidance
Screen and control access	X	X	Under CFATS, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. Under the MTSA program, facilities are to control access to the facility and designate and control access to restricted areas. All restricted areas are to have clearly established security measures to, among other things, identify which persons are authorized to have access and determine the conditions under which that access may take place.
Deter, detect, and delay	X	X	Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. Under the MTSA program, facilities are to deter the unauthorized introduction of dangerous substances and devices. They are also to monitor approaches and restricted areas as well as implement access control procedures. Further, facilities are also to implement security measures to prevent or deter unauthorized access to a restricted area.
Shipping, receipt, and storage	X	X	Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of quantity and physical location of hazmat. Under the MTSA program, the facility owner or operator must ensure that security measures relating to cargo handling are implemented in order to deter tampering. Further, facilities are required to create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances. In addition, facilities must, in general, coordinate enhanced security measures with shippers or other responsible parties.
Theft and diversion	X	X	Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. Under the MTSA program, storage areas for dangerous goods or hazardous substances are designated as restricted areas, and facilities must monitor and control access to these areas.
Sabotage	X	X	Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. Persons requiring unescorted access to secure areas generally must possess a Transportation Worker Identification Credential (TWIC) before such access is granted. The TWIC application process involves a security threat assessment. Further, at facilities with certain dangerous cargo, visitors, contractors, and other nonfacility employees must be escorted at all times while on the facility if access identification is not provided. Under MTSA, access to restricted areas is also controlled.

CFATS risk-based performance standard	CFATS	MTSA	Examples of program requirements and guidance
Cyber	X	X	Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. Under the MTSA program, facilities are to assess vulnerabilities of computer systems and networks as well as consideration of measures to protect radio and telecommunication equipment, including computer systems and networks. The Coast Guard recommends MTSA-regulated facilities refer to the cybersecurity framework information published by the National Institute of Standards and Technology when considering incorporation of cybersecurity measures into facility security plans.
Response	X	X	Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders. Under the MTSA program, the facility owner must ensure that facility security personnel are able to respond to security threats or breaches of security and maintain critical facility operations. Security incident procedures are to be included in facility security plans.
Monitoring	X	X	Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. Under the MTSA program, security systems—devices designed, installed, and operated to monitor, detect, observe, or communicate about activity that may pose a security threat—must be in good working order, regularly tested in accordance with the manufacturers' recommendations, noted deficiencies corrected promptly, and the results recorded. Further, facility security plans must include procedures for identifying and responding to security system and equipment failures or malfunctions.
Training	X	X	Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. Under the MTSA program, facility personnel must have knowledge of, through training or equivalent job experience, the facility security plan; recognition and detection of dangerous substances and devices; recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and techniques used to circumvent security measures, among other things. Further, facilities must conduct drills and exercises to test the proficiency of facility personnel in assigned security duties.
Employee background checks	X	X	Under the CFATS program, facilities must perform appropriate background checks for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. Under the MTSA program, employees requiring unescorted access to secure areas of the facility must obtain a TWIC, which includes undergoing a security threat assessment to check their criminal history and identify if they have terrorist ties, among other things.

CFATS risk-based performance standard	CFATS	MTSA	Examples of program requirements and guidance
Elevated threats	X	X	Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. Under the MTSA program, maritime facilities are required to take additional security precautions as the threat level rises as determined and announced by the Coast Guard. The Coast Guard has specified three maritime security (MARSEC) threat levels—MARSEC Level 1, 2, and 3—with 3 being the highest threat level).
Specific threats, vulnerabilities, or risks	X	X	Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment by, among other things, using new information and increasing security measures. Under the MTSA program, facility security plans must identify procedures to modify security measures for each MARSEC level.
Reporting of significant security incidents	X	X	Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. MTSA regulations include reporting requirements of suspicious activities, breaches in security, and transportation security incidents. Specifically, a facility is required to, without delay, report such activities or events to the Coast Guard National Response Center—an emergency call center that fields initial incident reports and forwards that information to appropriate federal or state agencies for response.
Significant security incidents and suspicious activities	X	X	Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this standard. The MTSA program requires that facility security personnel be able to respond to security threats or breaches of security, among other things. It also requires reporting of suspicious activity, breaches of security, and transportation security incidents to the National Response Center, and records maintained of any incidents.
Officials and organization	X	X	Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. The MTSA program requires facilities to identify a point of contact (the Facility Security Officer) that is responsible for implementing security actions at the facility, including ensuring the development and implementation of a facility security plan, adequate training for personnel performing facility security duties; and the maintenance of required records, among other things.
Records	X	X	Under the CFATS program, facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request. Under the MTSA program, facilities must keep records of (1) training, drills and exercises; (2) incidents and breaches of security; (3) actions taken in response to changes in MARSEC Levels; (4) maintenance and testing of security equipment; and (5) security audits, among other things.

Source: GAO analysis of CFATS and MTSA regulations and guidance. | GAO-21-12

The DOT hazardous materials transportation program. DOT requires certain safeguards for any product designated as a hazardous material and transported in certain quantities by rail, highway, air, or water. The hazardous materials transportation program is generally intended to improve public safety by preventing and mitigating hazardous materials transportation incidents and facilitating emergency response. Shippers (e.g., companies that could include multiple facilities) and carriers that transport certain hazardous materials are required to register with DOT. As of fiscal year 2019, there were about 14,000 shippers registered. According to our review of this registration data and DOT officials, the program could cover entities as diverse as chemical companies, large retailers, and research universities. The program requires certain facilities to develop and implement a security plan that must include an assessment of possible transportation security risks and appropriate measures to address the assessed risks.[13] At a minimum, the security plan must address personnel security, unauthorized access, and en route security. The security plan must also identify the senior management official responsible for implementing the plan, security duties for each employee or department responsible for implementing the plan, and a plan for training employees on the plan. Facilities are required to review their security plan at least annually and update it as necessary to reflect changing circumstances. We found that the hazardous materials (hazmat) transportation program contains requirements or guidance that generally align with almost all of the CFATS standards—16 of 18 (see table 7. “X” indicates that a program’s requirements or guidance generally align with the CFATS standard).

[13]See 49 C.F.R. § 172.802.

Table 7: Department of Transportation (DOT) Hazardous Materials (Hazmat) Transportation Requirements Program Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	DOT	Examples of program requirements and guidance
Restrict area perimeter	X	X	• Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. Facilities may consider using security measures to prevent unauthorized access such as security guards and surveillance cameras.
Secure site assets	X	X	• The CFATS program requires facilities to secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion detection systems. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. Facilities may consider using security measures to prevent unauthorized access such as securing hazardous materials in locked building or fenced areas and using tamper-resistant or tamper-evident seals and locks on cargo compartment openings.
Screen and control access	X	X	• Under CFATS, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. Facilities may consider using security measures to prevent unauthorized access such as restricting access to a single entry or gate and adding security guards.
Deter, detect, and delay	X	X	• Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. The plan must also address security risks of shipment of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement. Facilities may consider using security measures such as adding security guards and increase off-hour patrols by private security personnel, requesting that law enforcement personnel increase off-hour patrols, and considering equipping access gates with timed closure devices.

CFATS risk-based performance standard	CFATS	DOT	Examples of program requirements and guidance
Shipping, receipt, and storage	X	X	• Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of quantity and physical location of hazmat. • Under the DOT Hazmat program, facilities are to develop a plan that must include measures to address security risks of shipment of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement. Facilities may consider using security measures such as verifying the identity of the carrier and/or driver prior to loading hazardous materials and installing tamper-proof seals on all valves, package, or container openings. Facilities may also consider using advanced technology to track or protect shipments en route to their destinations, and establishing a communication system with transport vehicle and operators.
Theft and diversion	X	X	• Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. Facilities may consider security measures to prevent unauthorized access such as installing additional lights, alarm systems, or surveillance cameras and instituting a sign-out system for keys.
Sabotage	X	X	• Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. • Under the DOT Hazmat program, facilities are to develop a plan that includes measures to address the risk of unauthorized persons gaining access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials. The plans must also include measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan. The security plan must be available to employees who are responsible for implementing it, consistent with personnel security clearance restrictions and a demonstrated need to know.
Cyber	X	—	• Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. • DOT Hazmat regulations and guidance do not generally align with the CFATS Cybersecurity standard.

CFATS risk-based performance standard	CFATS	DOT	Examples of program requirements and guidance
Response	X	X	• Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders. • Under the DOT Hazmat program, facilities where hazardous materials are loaded for transportation, stored incidental to transportation or otherwise handled during any phase of transportation are required to maintain emergency response information, including a description of the hazardous material, whenever the hazardous material is present. This information must be in a location that is immediately accessible to facility personnel in the event of an incident involving the hazardous material.
Monitoring	X	—	• Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. • DOT Hazmat regulations and guidance do not generally align with the CFATS Monitoring standard.
Training	X	X	• Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. • Under the DOT Hazmat program, facilities must train employees whose employment directly affects hazardous materials transportation safety to recognize and respond to possible security threats, among other things. Employees that handle hazardous materials covered by the security plan, perform a regulated function related to the hazardous materials, or are responsible for implementing the plan must be trained concerning the security plan and its implementation. For example, such security training must include company security objectives, organizational security structure, specific security procedures, specific security duties and specific actions to be taken in the event of a security breach.
Employee background checks	X	X	• Under the CFATS program, facilities must perform appropriate background checks for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. • Under the DOT Hazmat program, facilities must take measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan. The security plan must be available to employees who are responsible for implementing it, consistent with personnel security clearance restrictions and a demonstrated need to know.
Elevated threats	X	X	• Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. • Under the DOT Hazmat program, specific measures put into place by the plan may vary commensurate with the level of threat at a particular time.

CFATS risk-based performance standard	CFATS	DOT	Examples of program requirements and guidance
Specific threats, vulnerabilities, or risks	X	X	• Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment by, among other things, using new information and increasing security measures. • Under the DOT Hazmat program, facility security plans must include an assessment of transportation security risks for shipments of the hazardous materials, including site-specific risks, and appropriate measures to address the assessed risks.
Reporting of significant security incidents	X	X	• Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. • Under the DOT Hazmat program, facilities may consider encouraging employees to report suspicious incidents or events, and may consider reporting suspicious incidents to the FBI and local law enforcement officials. Also, facilities must provide notice by telephone to the National Response Center as soon as practical but no later than 12 hours after of the occurrence of certain hazardous materials incidents, including the time and location of the incident, the extent of injury, and the nature of hazardous material involvement.
Significant security incidents and suspicious activities	X	X	• Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this standard. • Under the DOT Hazmat program, facilities may consider security measures such as keeping records of security incidents and reviewing records to identify trends and potential vulnerabilities. Facilities may also consider measures such as reporting suspicious incidents to the FBI and local law enforcement officials.
Officials and organization	X	X	• Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. • Under the DOT Hazmat program, facility security plans must include identification by job title of the senior management official responsible for overall development and implementation of the security plan. Facility security plans must also include security duties for each position or department that is responsible for implementing the plan or a portion of the plan and the process of notifying employees when specific elements of the security plan must be implemented.

CFATS risk-based performance standard	CFATS	DOT	Examples of program requirements and guidance
Records	X	X	• Under the CFATS program, facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request. • Under the DOT Hazmat program, facilities must retain for as long as in effect their security plans. The most recent version of the security plan, or portions thereof, must be available to the employees who are responsible for implementing it, consistent with personnel security clearance or background investigation restrictions and a demonstrated need to know. When the security plan is updated or revised, all employees responsible for implementing it must be notified and all copies of the plan must be maintained as of the date of the most recent revision. Each person required to develop and implement a security plan must maintain a copy of the security plan (or an electronic file thereof) that is accessible at, or through, its principal place of business and must make the security plan available upon request, at a reasonable time and location, to an authorized official of the Department of Transportation or the Department of Homeland Security.

Source: GAO analysis of CFATS and DOT regulations and guidance. | GAO-21-12

The RCRA program. EPA's program regulates the management of solid and hazardous waste from cradle to grave (i.e., from generation of the waste through disposal).[14] The goals set by the RCRA program, are, among others, to protect human health and the environment from the potential hazards of waste disposal and ensure that wastes are managed in an environmentally sound manner. Under its RCRA program, EPA has established standards applicable to hazardous waste generators and owners and operators of hazardous waste treatment, storage, and disposal facilities. As of March 2020, there were about 45,000 large quantity generators and about 700 treatment, storage, and disposal facilities, according to EPA data.[15] Requirements differ for facilities that generate waste (with more requirements for large quantity generators than small quantity generators), which are often chemical facilities that

[14]EPA has granted 48 states and some territories the authority to implement the RCRA program, according to EPA program officials. State RCRA programs must be at least as stringent as the federal requirements, but states can adopt more stringent requirements as well.

[15]Generators must generally: identify and count waste; comply with accumulation and storage requirements (including requirements for training and emergency arrangements); prepare the waste for transportation, track the shipment and receipt of such waste; and meet recordkeeping and reporting requirements, among other things.

may be subject to the CFATS program, according to EPA officials.[16] Further, hazardous waste treatment, storage, and disposal facilities have more security requirements than generators, and must obtain permits, according to EPA officials.[17] These officials stated that the purpose of the security measures is to restricting the public's access to hazardous wastes due to safety concerns, not to prevent terrorist acts. In addition, RCRA only regulates the part of the facility that is the "waste unit", where hazardous waste is stored, such as a drum storage area, not the entire facility. We found that the RCRA program contains requirements or guidance that generally align with 13 of the 18 CFATS program standards (see table 8. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

Table 8: Environmental Protection Agency (EPA) Resource Conservation and Recovery Act (RCRA) Hazardous Waste Management Requirements Program Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	RCRA	Examples of program requirements and guidance
Restrict area perimeter	X	X	• Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. • Under the RCRA program, Treatment, Disposal, and Storage Facilities (TSDFs) generally are to, among other things, prevent the unknowing entry, and minimize the possibility for the unauthorized entry, into the portion of the facility with hazardous waste operations (the active portion of the facility). For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility. TSDFs must also post signs reading "Danger-Unauthorized Personnel Keep Out" at every entrance to the active portion of the facility and at other locations, in sufficient numbers to be seen from any approach to the active portion.

[16]See 40 C.F.R. pt. 262. Hazardous waste generators may include various types of facilities and businesses ranging from large manufacturing operations, universities, and hospitals to small businesses, such as dry cleaners and auto body repair shops, and laboratories. Because these different types of facilities generate different quantities of wastes resulting in varying degrees of environmental risk, RCRA regulates generators based on the amount of waste that they generate in a calendar month. As a result, there are three categories of hazardous waste generators: large quantity generators; small quantity generators (SQGs); and conditionally exempt small quantity generators.

[17]See 40 C.F.R. pts. 264, 265.

CFATS risk-based performance standard	CFATS	RCRA	Examples of program requirements and guidance
Secure site assets	X	X	• The CFATS program requires facilities to secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion detection systems. • Under the RCRA program, TSDFs generally are to, among other things, prevent the unknowing entry, and minimize the possibility for the unauthorized entry, into the active portion of the facility. For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility. TSDFs must also post signs reading “Danger-Unauthorized Personnel Keep Out” at every entrance to the active portion of the facility and at other locations, in sufficient numbers to be seen from any approach to the active portion.
Screen and control access	X	X	• Under CFATS, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. • Under the RCRA program, TSDFs generally are to, among other things, prevent the unknowing entry, and minimize the possibility for the unauthorized entry, into the active portion of the facility. For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility. TSDFs must also post signs reading “Danger-Unauthorized Personnel Keep Out” at every entrance to the active portion of the facility and at other locations, in sufficient numbers to be seen from any approach to the active portion.
Deter, detect, and delay	X	X	• Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. • Under the RCRA program, TSDFs generally are to, among other things, prevent the unknowing entry, and minimize the possibility for the unauthorized entry, into the active portion of the facility. For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility. TSDFs must also post signs reading “Danger-Unauthorized Personnel Keep Out” at every entrance to the active portion of the facility and at other locations, in sufficient numbers to be seen from any approach to the active portion.
Shipping, receipt, and storage	X	X	• Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of quantity and physical location of hazmat. • Under the RCRA program, generators, transporters, and TSDFs are required to use a manifest system to track the movement of hazardous waste from the generator’s site to the site where the waste will be treated, stored, or disposed, and must include information about the waste such as the quantity, description of hazards, and EPA ID of the waste generator, transporter, and facility. Generators also have to comply with certain pre-transport requirements related to packaging, labeling, marking, and placarding.

CFATS risk-based performance standard	CFATS	RCRA	Examples of program requirements and guidance
Theft and diversion	X	X	• Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. • Under the RCRA program, TSDFs generally are to, among other things, prevent the unknowing entry, and minimize the possibility for the unauthorized entry, into the active portion of the facility. For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility. TSDFs must also post signs reading “Danger-Unauthorized Personnel Keep Out” at every entrance to the active portion of the facility and at other locations, in sufficient numbers to be seen from any approach to the active portion.
Sabotage	X	X	• Under the CFATS program, facilities must deter insider sabotage to prevent the facility’s property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. • Under the RCRA program, TSDFs generally are to, among other things, minimize the possibility for the unauthorized entry into the active portion of the facility. For example, TSDFs must install a 24-hour surveillance system that continuously monitors entry into the active area of the facility or a barrier that completely surrounds the active area of the facility and a means to control entry at all times through the gates or other entrances to the active portion of the facility.
Cyber	X	—	• Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. • RCRA program regulations and guidance do not address cybersecurity.
Response	X	X	• Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders. • Under the RCRA program, TSDFs are to, among other things, designate an emergency coordinator to guide emergency response activities, maintain a written contingency plan at the facility, and carry out that plan immediately in the event of an emergency. Generators must ensure that an emergency coordinator is on the premises, or on-call at all times, with responsibility for coordinating emergency response measures and attempt to make arrangements with local first responders and maintain records documenting such arrangements. Additionally, Large Quantity Generators are required to have written contingency plans.

CFATS risk-based performance standard	CFATS	RCRA	Examples of program requirements and guidance
Monitoring	X	X	• Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. • Under the RCRA program, generators and TSDFs generally must have an internal communications or alarm system capable of providing immediate emergency instruction to facility personnel, as well as a device capable of summoning emergency assistance, and such equipment must be tested and maintained.
Training	X	—	• Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. • Under the RCRA program, facilities are to ensure personnel complete specified training, but RCRA requirements or guidance do not include security training, exercises, and drills.
Employee background checks	X	—	• Under the CFATS program, facilities must perform appropriate background checks for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. • RCRA requirements or guidance do not generally align with the CFATS employee background checks standard.
Elevated threats	X	—	• Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. • RCRA requirements or guidance do not generally align with the CFATS elevated threats standard.
Specific threats, vulnerabilities, or risks	X	—	• Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment by, among other things, using new information and increasing security measures. • RCRA requirements or guidance do not generally align with the CFATS specific threats, vulnerabilities, or risks standard.
Reporting of significant security incidents	X	X	• Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. • Under the RCRA program, whenever there is an imminent or actual emergency situation, Large Quantity Generators and TSDFs must immediately notify appropriate state or local agencies with designated response roles if their help is needed. TSDFs must document events that required the implementation of the contingency plan, and within 15 days of the incident, the facility must submit a written report describing the incident to EPA.

CFATS risk-based performance standard	CFATS	RCRA	Examples of program requirements and guidance
Significant security incidents and suspicious activities	X	X	• Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this standard. • Under the RCRA program, whenever there is an imminent or actual emergency situation, Large Quantity Generators and TSDFs must immediately notify appropriate state or local agencies with designated response roles if their help is needed. TSDFs must document events that required the implementation of the contingency plan, and within 15 days of the incident, the facility must submit a written report describing the incident to EPA.
Officials and organization	X	X	• Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. • Under the RCRA program, generators and TSDFs are required to have an emergency coordinator who is responsible for coordinating all emergency response measures. The emergency coordinator must be thoroughly familiar with the facility's contingency plan, among other things. This requirement is not specific to officials and an organization responsible for security; however, the emergency coordinator is responsible for coordinating response measures, which may include response measures for security incidents.
Records	X	X	• Under the CFATS program, facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request. • Under the RCRA program, TSDFs must document events that required the implementation of the contingency plan, and within 15 days of the incident, the facility must submit a written report describing the incident to EPA.

Source: GAO analysis of CFATS and EPA regulations and guidance. | GAO-21-12

The Water Infrastructure Act program. The EPA's Water Infrastructure Act program requires the approximately 10,400 community water systems that each serve more than 3,300 people (about 7 percent of public water systems) to develop or update risk assessments and emergency response plans.[18] The focus of the assessments and plans is the risks of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals. The law specifies the components that the risk assessments and response plans must address, and establishes deadlines by which water systems must

[18]42 U.S.C. § 300i-2. The assessments and response plans are voluntary for public water systems serving fewer than 3,300 people and wastewater treatment facilities.

certify to EPA completion of the risk assessment and response plan.[19] EPA also provides guidance and an emergency response template that includes more detail and examples of measures that facilities may implement to satisfy the statutory requirements. Further, every 5 years, these water systems must review the risk assessment and submit a recertification to EPA that the assessment has been reviewed and, if necessary, revised. The law provides that the certification must contain only information that identifies the community water system submitting the certification, the date of the certification; and a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable,[20] and EPA officials stated that they do not review the risk assessment or independently verify the security measures listed in the emergency response plans. Based on our review of the Water Infrastructure Act and EPA guidance, we found that the Water Infrastructure Act program contains requirements or guidance that generally align with 10 of the 18 CFATS program standards (see table 9. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

The Risk Management Program. The purpose of the Risk Management Program is to prevent accidental releases of substances that can cause serious harm to the public and the environment from short-term exposures and to mitigate the severity of releases that do occur. Facilities holding more than a threshold quantity of a regulated hazardous substance in a process—of which there were about 12,000, according to EPA data as of January 2020—are required to comply with EPA's Risk Management Program regulations.[21] In general, risk management plans are to summarize the potential effects of accidental releases of certain chemicals, including an evaluation of the off-site effects of a worst-case

[19]Community water systems serving 100,000 or more are to certify their assessments by March 31, 2020; community water systems serving between 50,000 and 100,000 individuals by December 31, 2020; and community water systems serving between 3,300 and 50,000 individuals by June 30, 2021. 42 U.S.C. § 300i-2(a)(3)(A). Community water systems must develop emergency response plans within 6 months of their certification due dates. 42 U.S.C. § 300i-2(b). Of the 538 community water systems serving more than 100,000 people, 97 percent (519) met the March 31, 2020, statutory deadline, according to EPA. EPA officials stated that they continue to provide compliance assistance to the 19 systems that had not yet certified as of May 2020.

[20]33 U.S.C. § 300i-2(a)(4).

[21]40 C.F.R. § 68.10. EPA regulations define process as any activity involving a regulated substance, including any use, storage, manufacturing, handling, or on-site movement of such substances, or combination of these activities. 40 C.F.R. § 68.3.

release scenario, and the facility's emergency response program to prevent releases and mitigate any damage.[22] The Risk Management Program regulations were not designed to prevent release incidents caused by criminal activity, according to EPA officials. Nevertheless, certain provisions of the regulation may have the benefit of enhancing security and improving response to security-related incidents. We found that the Risk Management Program contains requirements or guidance that generally align with 13 of the 18 CFATS standards (see table 9. "X" indicates that a program's requirements or guidance generally align with the CFATS standard).

Table 9: America's Water Infrastructure Act (AWIA) Program and Risk Management Program (RMP) Alignment with Chemical Facility Anti-Terrorism Standards (CFATS)

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Restrict area perimeter	X	X	X	• Under the CFATS program, facilities must provide for a controlled perimeter surrounding the facility, or the restricted area(s) within a facility where critical assets are located, by securing and monitoring the perimeter of the facility or restricted areas. Security measures may include, for example, physical barriers, guard forces, electronic surveillance, or security lighting. • The AWIA program requires community water systems (water systems) to assess the resilience of physical barriers and to assess monitoring practices to malevolent threats and natural disasters. The Environmental Protection Agency's (EPA) risk assessment tool includes a list of countermeasures, including lighting and security cameras, that water systems can consider as part an optional step in their assessment. AWIA also requires community water systems to develop or update an emergency response plan that contains strategies and resources to improve the resilience of the water system, including physical security. Further, EPA guidance states that response plans should list restricted areas, such as chemical rooms, and who may access those areas. • Under RMP, certain facilities must develop and implement safe work practices to provide for the control of hazards during their operations, which may include control over entrance into the facility by employees.

[22]40 C.F.R. § 68.12. EPA has classified affected Risk Management Program processes into three distinct "Program Levels" to ensure that individual processes are subject to requirements that appropriately match their size and the risks they pose. As a result, different facilities covered by the regulations may have different requirements depending on their processes. Program Level 1 has the least stringent requirements of the three levels, whereas Program Level 3 has the most stringent requirements. Facilities regulated by Program Levels 1 and 2 of the Risk Management Program are subject to requirements or guidance that generally align with only five CFATS standards. For example, facilities with Program Level 1 processes are not required to develop an emergency response program.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Secure site assets	X	X	X	• Under the CFATS program, facilities must secure and monitor restricted areas or potentially critical targets (i.e., critical assets) within the facility. Security measures may include, for example, physical barriers, guard forces, or intrusion-detection systems. • The AWIA program requires water systems to develop or update an emergency response plan that contains strategies and resources to improve the resilience of the water system, including physical security. The EPA response plan template also states that plans should contain strategies that can aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of a water system, including physical security. For example, these detection strategies can include installing motion sensors and video cameras to monitor for facility break-ins or tampering. Further, EPA guidance states that response plans should list restricted areas, such as chemical rooms, and who may access those areas. • RMP requires certain facilities to develop and implement safe work practices to provide for the control of hazards during operations, such as control over entrance into the facility by employees. According to EPA, this RMP requirement is designed to secure assets in a manner that will control chemical process hazards at facilities.
Screen and control access	X	X	X	• Under the CFATS program, facilities must control access to the facility and to restricted areas within the facility through the identification, screening, and inspection of individuals and vehicles. • Under the AWIA program, water systems are required to develop or update an emergency response plan that contains strategies and resources to improve the resilience of the water system, including physical security. EPA guidance suggests that water systems document access control procedures in emergency response plans, such as that key cards are required to access all buildings. • Under RMP, certain facilities must develop and implement safe work practices to provide for the control of hazards during their operations, such as control of entrance into the facility by employees. According to the EPA, this requirement is intended to prevent inadvertent or unauthorized access entry to chemicals by support personnel whose jobs may not require such access.
Deter, detect, and delay	X	X	X	• Under the CFATS program, facilities must deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful. Security measures may include perimeter barriers, monitoring and detection systems, security lighting, and protective forces. • The AWIA program requires community water systems to develop or update an emergency response plan that includes strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system. • Under RMP, certain facilities must develop and implement safe work practices to provide for the control of hazards during their operations, such as control of entrance into the facility by employees.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Shipping, receipt, and storage	X	X	X	• Under the CFATS program, facilities must secure and monitor the shipping, receipt, and storage of hazardous materials to help a facility minimize the risk of theft or diversion of any of its hazardous materials. Security measures can include, for example, review procedures with redundancies for all shipping, receiving, and delivery of hazardous material (hazmat); lists of all hazmat at the facility; and tracking of the quantity and physical location of hazmat. • The AWIA program requires water systems to assess the use, storage, or handling of various chemicals to malevolent threats or natural disasters and incorporate the findings of the assessment in the system's emergency response plan. • Under RMP, certain facilities are required to develop and implement written operating procedures to address and provide clear instructions for the quality control of raw materials and for control of hazardous material inventories. According to EPA, this RMP requirement is designed to provide quality control of chemicals for safety and health considerations such as potential leaks or exposure to operators. EPA inspectors may view chemical delivery receipts, inventory lists, or equipment inspection logs to determine how chemical levels are monitored and managed.
Theft and diversion	X	X	X	• Under the CFATS program, facilities must deter the theft or diversion of potentially dangerous chemicals (e.g., chemical weapons, chemical weapons precursors, explosives, or other chemicals of interest that could be used to inflict harm at a facility or off-site). Security measures can include inventory controls, procedural measures such as access restrictions, and physical measures such as locks. • Under the AWIA program, water systems are to include strategies and resources to improve the resilience of the system, including the physical security of the system, in their emergency response plan. Further, EPA guidance states that response plans should list restricted areas, such as chemical rooms, and who may access those areas. • Under RMP, certain facilities must develop and implement safe work practices to provide for the control of hazards during their operations, such as control of entrance into the facility by employees. According to the EPA, this requirement is intended to prevent inadvertent or unauthorized entry to chemicals by support personnel whose jobs may not require such access.
Sabotage	X	X	X	• Under the CFATS program, facilities must deter insider sabotage to prevent the facility's property and activities from being used by a potential terrorist against the facility through, among other things, background checks, visitor controls, administrative controls and physical security measures, and cybersecurity measures. • Under AWIA, water systems are to include strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system, in their emergency response plan. Further, EPA guidance states that response plans should list restricted areas, such as chemical rooms, and who may access those areas. • Under RMP, certain facilities must develop and implement safe work practices to provide for the control of hazards during their operations, such as control of entrance into the facility by employees. According to the EPA, this requirement is intended to prevent inadvertent or unauthorized entry to chemicals by support personnel whose jobs may not require such access.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Cyber	X	X	—	• Under the CFATS program, facilities must deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls—such as Supervisory Control and Data Acquisition systems, Distributed Control Systems, Process Control Systems, Industrial Control Systems, critical business systems, and other sensitive computerized systems—through a combination of policies and practices that include, among other things, security policies, access controls, personnel security, and awareness and training. • The AWIA program requires water systems to assess the resilience of computer or other automated systems to malevolent threats and natural disasters. AWIA also requires water systems to develop an emergency response plan that includes strategies and resources to improve the resilience of the system, including cybersecurity. • RMP regulations and guidance do not address cybersecurity.
Response	X	X	X	• Under the CFATS program, facilities must develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders. • The AWIA program requires water systems to develop an emergency response plan that incorporates the findings of the risk assessment. AWIA also requires these systems to coordinate with existing local emergency response planning committees in developing their risk assessment and response plan. • Under RMP, facilities are required to coordinate response needs with local emergency response agencies and have appropriate mechanisms in place to notify emergency responders when there is a need for a response. Also, certain facilities must develop an emergency response program for the purpose of protecting public health and the environment, including a plan to respond to accidental chemical releases.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Monitoring	X	X	X	• Under the CFATS program, facilities must maintain effective monitoring, communications, and warning systems, which will allow facilities to notify internal personnel and local responders in a timely manner about security incidents. Specifically, facilities must implement measures designed to (1) ensure that security systems and equipment are in good working order; (2) regularly test security systems; and (3) identify and respond to security system failures or malfunctions. • The AWIA program requires water systems to assess the resilience of monitoring practices, which, according to EPA officials, means the processes and practices used to monitor source water and finished water quality. However, AWIA also requires water systems to include in their emergency response plan strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system. Guidance suggests that air monitors, such as for chlorine gas, can alert personnel to any leaks in a timely fashion. It also suggests that intrusion detection systems should be properly installed and maintained. EPA guidance further suggests that water systems should inventory and track all communication equipment to help ensure maintenance is scheduled as appropriate and that equipment replacement can be planned. • Under RMP, certain facilities must develop and implement written operating procedures that address safety systems and their functions. Also, certain facilities must take specific actions to maintain the mechanical integrity of process equipment, such as controls, including monitoring devices and sensors, alarms, and interlocks. Further, emergency response programs required for certain facilities must include development of an emergency response plan that includes procedures for the use of emergency response equipment and for its inspection, testing, and maintenance.
Training	X	—	—	• Under the CFATS program, facilities must ensure proper security and response training, exercise, and drills of facility personnel so they are better able to identify and respond to suspicious behavior, attempts to enter or attack a facility, or other malevolent acts by insiders or intruders. • AWIA, RMP requirements, and associated EPA guidance do not address security training, exercises, and drills.
Employee background checks	X	—	—	• Under the CFATS program, facilities must perform appropriate background checks for facility personnel and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including 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. • AWIA, RMP requirements, and associated EPA guidance do not address employee background checks.
Elevated threats	X	—	—	• Under the CFATS program, facilities must escalate the level of protective measures for periods of elevated threat by, among other things, increasing security measures to better protect against known increased threats or generalized increased threat levels declared by the federal government. • AWIA, RMP regulations, and associated EPA guidance do not address escalating the level of protective measures for periods of elevated threats.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Specific threats, vulnerabilities, or risks	X	—	—	• Under the CFATS program, facilities must address specific threats, vulnerabilities, or risks identified for the particular facility, such as those not identified in the facility's security vulnerability assessment, by, among other things, using new information and increasing security measures. • AWIA, RMP requirements, and associated EPA guidance do not address specific threats, vulnerabilities, or risks that are new or may not have been previously identified.
Reporting of significant security incidents	X	—	X	• Under the CFATS program, facilities must report significant security incidents to the Department of Homeland Security (DHS) and to local law enforcement officials. According to CFATS guidance, the facility should have a process or written procedures in place to rapidly and efficiently report security incidents to the appropriate entities. • AWIA does not require and EPA guidance does not address reporting of significant security incidents. However, according to EPA officials, this standard could be addressed within a water system's emergency response plan. EPA's template for emergency response plans includes a section devoted to coordination with law enforcement and external partners. The template also recommends that water systems describe or reference their procedures for working with law enforcement officials if an incident is declared a crime scene. • RMP requires facilities to include in their RMP a 5-year accident history of all accidental chemical releases that resulted in deaths, injuries, or significant property damage on site or known offside deaths, injuries, evacuations, sheltering in place, property damage, or environmental damage. According to EPA, while this requirement does not specifically require facilities to report significant security incidents, some facilities may include security incidents if they result in an accidental release.
Significant security incidents and suspicious activities	X	—	X	• Under the CFATS program, facilities must identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site. According to CFATS guidance, facilities should have documented processes and procedures addressing this CFATS standard. • AWIA does not require and EPA guidance does not address identifying, investigating, and maintaining records of significant security incidents and suspicious activities. However, according to EPA, this CFATS standard, though not required under AWIA, could be addressed within a water system's emergency response plan. EPA's template for emergency response plans includes a section devoted to coordination with law enforcement. • Under RMP, certain facilities are required to investigate each incident that resulted in, or could reasonably have resulted in a catastrophic chemical release which is a major uncontrolled emission, fire, or explosion, involving one or more regulated substances that presents imminent and substantial endangerment to public health and the environment. They must also retain incident investigation reports for 5 years. While this requirement is not specific to security incidents, some facilities may include security incidents in their RMP incident investigation program if they result in or could reasonably have resulted in a catastrophic release, according to EPA.

CFATS risk-based performance standard	CFATS	AWIA	RMP	Examples of program requirements and guidance
Officials and organization	X	—	X	• Under the CFATS program, facilities must establish official(s) and an organization responsible for security and for compliance with CFATS. DHS generally anticipates that each facility will identify a Facility Security Officer as well as a facility security organization responsible for implementing the facility security plan. • AWIA and associated guidance do not address the identification of officials or organizations responsible for security and compliance. This CFATS standard, though not required under AWIA, could be addressed within a water system's emergency response plan. EPA's template for emergency response plans includes a section devoted to incident command system roles and emergency response roles. • RMP requires facilities to assign a qualified person or position that has the overall responsibility for the development, implementation, and integration of the risk management program elements. While this requirement is not specifically intended to establish officials and an organization responsible for security, some facilities may include these under their RMP management system if the role also relates to complying with the RMP provisions for chemical accident prevention, according to EPA.
Records	X	—	X	• Under the CFATS program, facilities must maintain appropriate records that address the creation, maintenance, protection, storage, and disposal of appropriate security-related records and the activities required to make these records available to DHS upon request. • AWIA and associated EPA guidance do not address the maintenance of security-related records. • RMP requires facilities to maintain records supporting the implementation of the program for 5 years. According to EPA, while this requirement does not specifically require RMP facilities to maintain security records, some facilities may maintain some form of security records within their RMP records if the information is also associated with complying with the RMP provisions.

Source: GAO analysis of statutes and DHS and EPA regulations and guidance. | GAO-21-12

Appendix III: Comments from the Department of Homeland Security

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

Homeland Security

December 17, 2020

Nathan Anderson
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-21-12 "CHEMICAL SECURITY: Overlapping Programs Could Better Collaborate to Share Information and Identify Potential Security Gaps"

Dear Mr. Anderson:

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

The Department is pleased to note GAO's recognition of the comprehensive security requirements contained within the Chemical Facility Anti-Terrorism Standards (CFATS) regulations. The U.S. has thousands of facilities that produce, use, or store hazardous chemicals that, if not properly safeguarded, could possibly be used by terrorists to inflict mass casualties and damage, and approximately 3,300 of those facilities are required to develop and implement comprehensive security plans pursuant to CFATS. As approximately 16 percent, or about 550, of the 3,300 facilities subject to CFATS regulations are also regulated by other federal Departments and Agencies, the Department agrees that this may result in some regulatory overlap and duplication.

However, DHS believes the actual impact on facilities is less significant than implied by GAO for two primary reasons. First, GAO overestimates the overlap in actual requirements imposed by CFATS and those of programs that GAO found to "generally align" with CFATS, with GAO frequently claiming "general alignment" exists when, in fact, the regulation being compared to CFATS requires activities that satisfy only a small portion of the specific CFATS risk-based performance standard being evaluated. Secondly, GAO underestimates the reduction in the potential impact of any regulatory overlap alleviated by CFATS allowing facilities to use activities performed in response to other regulations for compliance with CFATS.

The Department also notes GAO's recognition of the May 2014 report "Actions to Improve Chemical Facility Safety and Security—A Shared Commitment" co-authored by DHS pursuant to the "Executive Order on Improving Chemical Facility Safety and Security" (EO 13650), and the steps taken consistent with it to both modernize policies, regulations, and standards while also improving interagency coordination and information sharing. In 2018, DHS and its partner Departments and Agencies executed an updated charter, which reaffirms our commitment to the principles and activities to minimize potential conflicts and overlap advocated in the 2014 report. DHS looks forward to continuing work with other Departments and Agencies to ensure chemical facilities are properly secured while minimizing any potential overlap, duplication, and fragmentation. DHS remains committed to not only ensuring that high-risk chemical facilities are implementing appropriate security measures, but also to collaborating with other federal Departments and Agencies with regulatory oversight of chemical facility security and safety to minimize regulatory overlap, duplication, and fragmentation.

The draft report contained seven recommendations, including three for DHS with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing accuracy and contextual issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2020.12.17 13:57:41 -05'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-21-12

GAO recommended that the Secretary of DHS:

Recommendation 1: Direct its chemical safety and security programs to collaborate with partners and establish an iterative and ongoing process to identify the extent to which CFATS-regulated facilities are also covered by other programs with requirements or guidance that generally align with some CFATS standards.

Response: Concur. The Department believes that reviewing the extent to which CFATS-regulated facilities are also covered by other programs with requirements or guidance that generally align with some CFATS standards in an iterative, ongoing manner will allow DHS and partner federal agencies to further reduce potential overlap and duplication, and better identify possible security gaps between regulatory regimes.

To achieve this, DHS Cybersecurity and Infrastructure Security Agency's (CISA) Infrastructure Security Division (ISD) will continue to lead the Department's routine collaboration with fellow federal agencies with chemical safety or security responsibilities through the Chemical Government Coordinating Council, the working group established to implement EO 13650, and direct one-on-one engagements as necessary. Additionally, CISA ISD will develop and implement of a plan of action or similar document detailing an iterative and ongoing process for identifying the extent to which CFATS-regulated facilities are also covered by other programs with requirements or guidance that generally align with some CFATS standards. Estimated Completion Date (ECD): December 31, 2021.

GAO recommended that the Director of CISA:

Recommendation 5: Update CFATS program guidance or fact sheets to include a list of commonly accepted actions facilities may have taken and information they may have prepared pursuant to other federal programs and disseminate this information.

Response: Concur. As demonstrated by CISA ISD's issuance of numerous CFATS-related fact sheets and other guidance materials, DHS recognizes the value these materials can provide to a regulated community. ISD further believes that, by providing guidance on actions or information a facility may be able to reuse containing regulations or guidance that generally align with some aspect of CFATS for the purposes of CFATS compliance, ISD may reduce potential duplication and overall regulatory burden. Consequently, ISD will update or create a new guidance document or fact sheet that includes a list of commonly accepted actions CFATS-regulated facilities may have taken and information they may have prepared pursuant to other federal programs and disseminate this information.

3

As part of this effort, ISD will review regulatory requirements from complimentary chemical safety and security programs, as well as a sampling of approved CFATS site security plans relying in part on measures or information also used for compliance with other chemical safety or security regulatory regimes. Additionally, ISD will solicit inputs from the federal partners responsible for implementing complimentary regulatory programs, and representatives from the regulated community on actions CFATS-regulated facilities have taken and information they have prepared pursuant to other federal programs, that might be applicable to CFATS compliance. ECD: December 31, 2021.

Recommendation 6: Collaborate with the EPA [Environmental Protection Agency] to assess the extent to which potential security gaps exist at water and wastewater facilities and, if gaps exist, develop a proposal for how best to address them and submit it to the Secretary of Homeland Security and Administrator of EPA, and Congress, as appropriate.

Response: Concur. Although DHS previously noted the existence of security gaps at water and wastewater (W/WW) facilities which are exempt from CFATS and generally not mandated to maintain comprehensive security postures under another regulatory regime, ISD will work with EPA to identify and explore possible approaches for assessing potential security gaps that exist at W/WW facilities broadly. Approaches utilized might include, among other things: 1) an in-house review of existing W/WW facility regulatory and voluntary submissions; or 2) the funding of a third-party study on the issue. This assessment will be used to determine what, if any, additional actions are warranted, and is anticipated to be complete by July 29, 2022.

Based on the results of the assessment described in the previous paragraph, ISD and the EPA will determine if any additional action is warranted. If it is determined that a significant security gap exists, ISD and EPA will identify and evaluate potential options for addressing that gap. Specifically, one option under consideration would be to work with Congress to legislatively address the gap either through: 1) the removal of the existing W/WW facility exemption from CFATS; or 2) by providing either DHS or EPA with new authority to regulate security at these facilities. Alternatively, DHS or EPA could seek to address the gap through an expansion of existing or new voluntary security programs, including the: 1) provision by CISA Chemical Security Inspectors to W/WW facilities of elements of CISA's emerging suite of voluntary chemical security offerings; 2) increased engagement with W/WW facilities by CISA Protective Security Advisors; or 3) development of new voluntary programs within EPA's Water Security Division. Given the large number of W/WW facilities, and the fact that these programs' existing resources are currently fully utilized, any of these approaches are likely to require Congress to allocate additional resources for them to be successful. ISD anticipates selecting an approach based on the results of the assessment by October 31, 2022. Overall ECD: To Be Determined.

4

Appendix IV: Comments from the Department of Transportation

U.S. Department of Transportation
Office of the Secretary of Transportation

Assistant Secretary for Administration

1200 New Jersey Avenue, SE
Washington, DC 20590

December 15, 2020

Nathan Anderson
Director, Homeland Security and Justice
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

Dear Mr. Anderson:

The mission of the U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) is to protect people and the environment by advancing the safe transportation of energy and other hazardous materials that are essential to our daily lives. PHMSA is committed to ensuring the safe and secure transportation of all hazardous materials. PHMSA has on-going discussions with chemical safety and security partners within the industry and other governmental agencies. These discussions include examining how PHMSA's hazardous materials safety and security requirements complement other programs and requirements.

Upon review of the GAO's draft report, we concur with the recommendation to collaborate with other regulatory agencies and identify the extent to which facilities required to comply with the hazardous materials regulations are also covered by the Chemical Facility Anti-Terrorism Standards program. We will provide a detailed response to this recommendation within 180 days of the final report's issuance.

We appreciate the opportunity to respond to the GAO draft report. Please contact Madeline M. Chulumovich, Director, Audit Relations and Program Improvement, at (202) 366-6512 with any questions.

Sincerely,

Keith Washington
Deputy Assistant Secretary for Administration

Appendix V: Comments from the Environmental Protection Agency

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF THE ADMINISTRATOR

December 18, 2020

Nathan Anderson
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Anderson:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's (GAO) draft report "Chemical Security: Overlapping Programs Could Better Collaborate to Share Information and Identify Potential Security Gaps" (GAO-21-12).

The U.S. Environmental Protection Agency acknowledges that efforts to minimize overlap, duplication and fragmentation of regulatory requirements for facilities may reduce the burden for regulated facilities, and improving coordination between EPA and the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) can help achieve this goal. To that end, EPA is committed to collaborating with DHS to address potential security gaps identified in the Chemical Facility Anti-Terrorism Standard (CFATS) program.

The regulatory programs identified by GAO in the draft report, namely the Risk Management Program (RMP), the Resource Conservation and Recovery Act (RCRA) program and the America's Water Infrastructure Act (AWIA) program, are administered by the Office of Land and Emergency Management (OLEM) and the Office of Water (OW). The GAO made two recommendations to EPA, for which OLEM will serve as the lead for Recommendation 2, while OW will serve as the lead in addressing Recommendation 7.

The following provides the Agency's response to GAO's recommendations:

GAO Recommendation 2: The Administrator of the EPA should direct its chemical safety and security programs to collaborate with partners and establish an iterative and ongoing process to identify the extent to which the facilities that it regulates are also covered by the CFATS program.

EPA Response: The Agency agrees with the recommendation and that collaboration between DHS and EPA will lead to improved chemical security programs and commits to continued coordination with DHS to provide relevant Agency information to the CFATS program. By ensuring this partnership is ongoing and iterative, both EPA and DHS will benefit from improved communication between the two agencies.

EPA commits to developing a workplan with DHS which will document the agreed-upon process for the ongoing exchange in information. Collaboration in an ongoing manner may take several forms, including the continuation of activities related to the national working group established by the *Executive Order on Improving Chemical Facility Safety and Security* (Executive Order 13650). Tentatively, the Agency anticipates additional activities will include information sharing of facility data, information relating to relevant enforcement actions, and Agency regulatory information. EPA will begin implementing the plan by December 31, 2021.

GAO Recommendation 7: The EPA should collaborate with the DHS's Cybersecurity and Infrastructure Agency to assess the extent to which potential security gaps exist at water and wastewater facilities and, if gaps exist, develop a legislative proposal for how best to address them and submit it to the Security of Homeland Security and Administrator of EPA, and Congress, as appropriate.

EPA Response: EPA does not concur with the recommendation as written. The GAO report already provides a detailed analysis that the two agencies can use as a starting point for discussion. On the recommendation to submit a legislative proposal, this recommendation is unnecessary and inappropriate. It is unnecessary because EPA and DHS have already provided testimony to Congress that a security gap exists and the gap should be addressed. EPA provided testimony both during the George W. Bush Administration and during the Obama Administration (see attached EPA testimony).[1] In addition, a recommendation for EPA to develop a legislative proposal is inappropriate because the Legislative Branch develops legislation—not the Executive Branch.

The Agency agrees with GAO's recommendation to collaborate across Federal agencies to address potential security gaps and regularly engages with CISA, and proposes the following revisions to the recommendation to reflect the work EPA can commit to complete in support of this effort:

[1] Links to full record of congressional hearings:
https://www.govinfo.gov/content/pkg/CHRG-110hhrg46861/pdf/CHRG-110hhrg46861.pdf
https://www.govinfo.gov/content/pkg/CHRG-111shrg56889/pdf/CHRG-111shrg56889.pdf
https://www.govinfo.gov/content/pkg/CHRG-111shrg23573/pdf/CHRG-111shrg23573.pdf

Proposed revision to GAO Recommendation 7: The EPA should collaborate with DHS CISA to discuss the GAO report findings on the extent to which potential security gaps exist at water and wastewater facilities and identify ways to best address the gaps under current authorities as appropriate.

EPA appreciates the opportunity to review the GAO draft report. If you have any questions, please contact Sue Perkins in the Office of the Chief Financial Officer at (202) 564-8618 or Perkins.Susan@epa.gov.

Sincerely,

Doug Benevento

Doug Benevento
Associate Deputy Administrator

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Nathan Anderson, (206) 287-4804 or andersonn@gao.gov.

Staff Acknowledgments

In addition to the contact above, Ben Atwater (Assistant Director), Andrew Curry (Analyst-in-Charge), Ben Crossley, Dominick Dale, David Dornisch, Michele Fejfar, Paul Hobart, Andrew Kincare, Tracey King, Ryan Lester, Tom Lombardi, Grant Mallie, and Dennis Mayo made key contributions.