United States Government Accountability Office

Report to Congressional Requesters

May 2020

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

GAO-20-453

GAO Highlights

Highlights of GAO-20-453, a report to congressional requesters

May 2020

CRITICAL INFRASTRUCTURE PROTECTION

Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities

Why GAO Did This Study

Thousands of high-risk chemical facilities may be subject to the risk posed by cyber threat adversaries—terrorists, criminals, or nations. These adversaries could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict mass causalities to surrounding populations (see figure). In accordance with the DHS Appropriations Act, 2007, DHS established the CFATS program to, among other things, identify and assess the security risk posed to chemical facilities.

GAO was asked to examine the cybersecurity efforts of the CFATS program, including the extent to which the program (1) assesses the cybersecurity efforts of covered facilities, and (2) determines the specialty training and level of staff needed to assess cybersecurity at covered facilities.

GAO conducted site visits to observe the cybersecurity portion of CFATS inspections based on scheduled inspections, reviewed inspection documents, and interviewed CFATS inspectors. GAO also analyzed inspection guidance and training against key practices and assessed workforce planning documents and processes.

What GAO Recommends

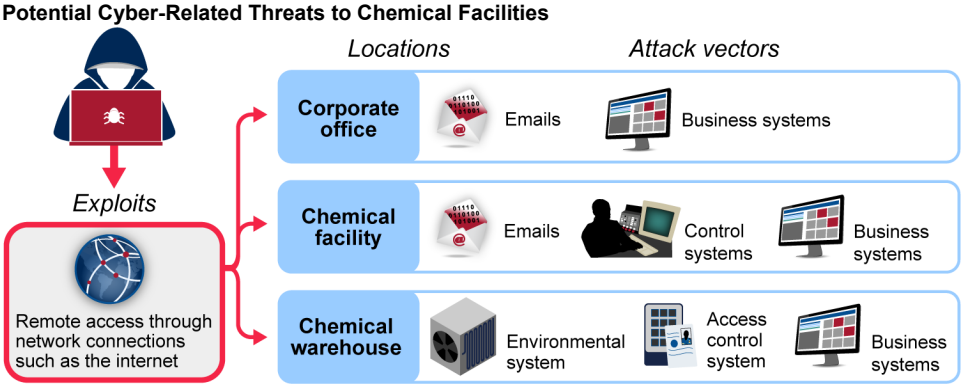
GAO is making six recommendations to DHS to routinely review guidance and update, as needed; to fully incorporate key training practices; and to identify workforce cybersecurity needs. DHS concurred with the recommendations.

View GAO-20-453. For more information, contact Nathan Anderson at (206) 287-4804 or andersonn@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Chemical Facility Anti-Terrorism Standards (CFATS) program within the Department of Homeland Security (DHS) evaluates high-risk chemical facilities' cybersecurity efforts via inspections that include reviewing policies and procedures, interviewing relevant officials, and verifying facilities' implementation of agreed-upon security measures. GAO found that the CFATS program has guidance designed to help the estimated 3,300 CFATS-covered facilities comply with cybersecurity and other standards, but the guidance has not been updated in more than 10 years, in contrast with internal control standards which recommend periodic review. CFATS officials stated that the program does not have a process to routinely review its cybersecurity guidance to ensure that it is up to date with current threats and technological advances. Without such a process, facilities could be more vulnerable to cyber-related threats.

Potential Cyber-Related Threats to Chemical Facilities



Source: GAO analysis of potential cybersecurity threats to chemical facilities. | GAO-20-453

The CFATS program developed and provided cybersecurity training for its inspectors, but GAO found that the CFATS program does not fully address 3 of 4 key training practices, or address cybersecurity needs in its workforce planning process, as recommended by DHS guidance. Specifically:

- The CFATS program does not: (1) systematically collect or track data related to inspectors' cybersecurity training or knowledge, skills, and abilities; (2) develop measures to assess how training is contributing to cybersecurity-related program results; or (3) have a process to evaluate the effectiveness of its cybersecurity training in improving inspector skillsets.
- The program also has yet to incorporate identified cybersecurity knowledge, skills, and abilities for inspectors in its current workforce planning processes or track data related to covered facilities' reliance on information systems when assessing its workforce needs.

Fully addressing key training practices will help ensure that CFATS inspectors have the knowledge, skills, and abilities for cybersecurity inspections, and identifying cybersecurity needs in workforce planning will help the program ensure that it has the appropriate number of staff to carry out the program's cybersecurity-related efforts.

Contents

Abbreviations

CFATS	Chemical Facility Anti-Terrorism Standards
COI	chemical of interest
DHS	Department of Homeland Security
FTE	full-time equivalent
IT	information technology
NIST Cybersecurity Framework	National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
SCADA	Supervisory Control and Data Acquisition systems

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

May 14, 2020

Congressional Requesters

Thousands of facilities that produce, use, or store hazardous chemicals could be targeted or used by terrorists in an effort to inflict mass causalities, damage, and fear. These chemicals could be released from a facility to cause harm to surrounding populations or they could be stolen and used as chemical weapons or as their precursors (the ingredients for making chemical weapons). In addition, as reliance on information systems continues to increase, cyber-based threat adversaries—such as terrorists, criminals, or nations—could maliciously manipulate an organization's physical security, information, and process control systems to steal chemicals or to cause harm through release or explosion.[1] For example, the Department of Energy's Idaho National Laboratory reported in 2018 that malicious actors targeted a Middle Eastern company's industrial safety systems with the intention to disrupt the industrial control system, allow attackers to gain access to safety systems, and modify safety processes that could have been physically dangerous or cause harm to people.[2]

The Chemical Facility Anti-Terrorism Standards (CFATS) program is intended to ensure the security of the nation's chemical infrastructure. Pursuant to the Department of Homeland Security (DHS) Appropriations Act, 2007, DHS established the CFATS program to, among other things, identify high-risk chemical facilities and assess the risk posed by each; place facilities identified as high-risk into one of four risk-based tiers; and assess, approve, and inspect facility security measures to ensure

[1]Process control systems is a collective term used to describe different types of controls systems, which include the devices, systems, networks, and controls used to operate or automate industrial processes. Examples of these systems include Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, process control systems (PCS), and industrial control systems. These systems may be used to simply monitor processes—for example, the environmental conditions in a small office building—or to manage the complex activities of a chemical manufacturing plant. Process control systems are vulnerable to cyberattack from inside and outside the control system network.

[2]Department of Energy's Idaho National Laboratory, *History of Industrial Control System Cyber Incidents*, INL/CON-18-44411-Revision-2 (Washington, D.C.: December 2018).

compliance with regulatory requirements.[3] Chemical facilities that DHS determines to meet the risk criteria are called covered chemical facilities.[4] Facilities' cybersecurity measures are specifically inspected and assessed under the CFATS program, when applicable. The Infrastructure Security Compliance Division within DHS's Cybersecurity and Infrastructure Security Agency manages the CFATS program.[5]

We previously reported on various aspects of the CFATS program and identified challenges DHS was experiencing in implementing and managing the program.[6] Although there have been program improvements in recent years, questions remain about the progress DHS has made in implementing changes to the program and the extent to which the CFATS program is ensuring that the highest-risk chemical facilities are more secure as a result. In August 2018, we recommended that DHS track vulnerability reduction from the implementation and verification of security efforts, including cybersecurity measures, at the high-risk chemical facilities that CFATS regulates.[7] In September 2018, we included in our 2018 high-risk series report on cybersecurity issues facing the nation that DHS's new performance measure methodology for

[3]See 72 Fed. Reg 17,688 (Apr. 9, 2007) (codified as amended at 6 C.F.R. pt. 27); see also Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388-89 (2006). The high-risk determination is based on a risk assessment methodology that calculates risk scores using facility-supplied information, among other sources, and takes into account vulnerability, potential consequences, and the threat of a terrorist attack.

[4]6 U.S.C. § 621(3).

[5]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 imposing additional implementation requirements on DHS for the program. See Pub. L. No. 113-254, 128 Stat. 2898 (2014); 6 U.S.C. §§ 621-629. 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 repealing the program's authority under the fiscal year 2007 DHS appropriations act. In January 2019, the Chemical Facility Anti-Terrorism Standards Program Extension Act was enacted and extended the authorization by 15 months. Pub. L. No. 116-2, 133 Stat. 5 (2019).

[6]GAO, *Critical Infrastructure Protection: DHS Actions Needed to Verify Some Chemical Facilities' Information and Manage Compliance Process*, GAO-15-614 (Washington, D.C.: July 2015) and GAO, *Critical Infrastructure Protection: Progress and Challenges in DHS's Management of its Chemical Security Program*, GAO-19-402T (Washington, D.C.: February 27, 2019).

[7]GAO, *Critical Infrastructure Protection: DHS Should Take Actions to Measure Reduction in Chemical Facility Vulnerability and Share Information with First Responders*, GAO-18-538 (Washington, D.C.: August 2018).

CFATS did not measure reduction in vulnerability at a facility resulting from the implementation and verification of planned security measures during the compliance inspection process.[8] As of April 2020, this recommendation remains open and we continue to monitor DHS efforts to address it.[9]

In addition, we reported that companies in the chemical sector had increasingly sought to gain efficiencies by connecting their physical security, information, and process control systems. However, we found that the convergence between these systems was a major challenge for owners and operators of critical infrastructure, including chemical manufacturing facilities, as it created new opportunities for potential cyber adversaries to access these systems.[10]

You asked us to examine the cybersecurity efforts of the CFATS program. This report addresses the extent to which the CFATS program (1) assesses the cybersecurity efforts of CFATS-covered chemical facilities and (2) determines the level of specialty training and staff needed to assess cybersecurity at covered chemical facilities.

To address both of our objectives, we conducted site visits to two chemical facilities out of the five inspections scheduled for facilities with an elevated level of cybersecurity risk during the data-gathering period of our audit. During these site visits, we observed the cybersecurity portion of CFATS inspections in two of the 10 CFATS program regions. We selected the facilities and regions based on the program's inspection schedule availability from September 2019 through January 2020. The results of these site visits cannot be generalized to all inspections at covered facilities, although they provided us with important context on the questions inspectors ask and observations and processes that they perform during their review of facilities' physical security, information, and process control systems and related policies.

[8]GAO, *High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: September 2018).

[9]GAO, *Critical Infrastructure Protection: Progress and Challenges in DHS's Management of its Chemical Facility Security Program*, GAO-19-402T (Washington, D.C.: February 2019); and GAO-18-538.

[10]GAO, *Critical Infrastructure Protection: DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning*, GAO-18-62 (Washington, D.C.: October 2017).

To determine the extent to which the CFATS program assesses the cybersecurity efforts of covered chemical facilities, we examined the program's inspection handbooks; guidance materials, including the Risk-Based Performance Standards Guidance[11] known as the CFATS guidance in this report; and standard operating procedures used to review the cybersecurity posture of covered chemical facilities to ensure their compliance with the cybersecurity standard.[12] We also obtained selected CFATS inspection and facility approval reports to review how inspectors documented the implementation of a facility's cybersecurity measures and any changes to a facility's information and process control systems.[13] We assessed DHS's efforts to evaluate the program's cybersecurity guidance against the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) and other DHS and chemical industry cybersecurity guidelines to evaluate the extent to which the program's cybersecurity guidance took into account evolving cybersecurity threats and mitigation strategies.[14]

We also interviewed representatives from five chemical industry associations and two chemical companies to obtain their perspectives on the CFATS program's cybersecurity guidance and approval and inspection processes as well as other standards used to mitigate cybersecurity risks at chemical facilities.[15] We selected chemical industry

[11]Department of Homeland Security, *Risk-Based Performance Standards Guidance, Chemical Facility Anti-Terrorism Standards* (Washington, D.C.; May 2009).

[12]The cybersecurity standard states, "deter cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls, such as SCADA systems, distributed control systems, process control systems, and industrial control systems; critical business systems; and other sensitive computerized systems." 6 C.F.R. § 27.230(a)(8).

[13]As discussed later in this report, CFATS officials manually selected inspection reports for our review because there was no systematic way to extract reports from the program's database that represented covered facilities with varying reliance on information and process control systems.

[14]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, M.D.: April 2018). Department of Homeland Security, *Chemical Sector Cybersecurity Framework Implementation Guidance* (Washington, D.C.: 2015).

[15]We interviewed representatives from the American Chemistry Council, The Chlorine Institute, Institute of Makers of Explosives, National Association of Chemical Distributors, Society of Chemical Manufacturers and Affiliates, DOW Chemical Company, and BASF Corporation.

associations that were members of DHS's Chemical Sector Coordination Council and to reflect a range of chemical facility types, such as chemical and explosives manufacturers. We interviewed CFATS officials at headquarters, two managers and two CFATS inspectors from the two program regions we visited, and two cyber analysts to better understand the program's cybersecurity guidance, inspection and approval processes, and performance measures. During our site visits to the two chemical facilities, we also discussed inspector roles and responsibilities and inspection processes with the same two CFATS inspectors.

To determine the extent to which the CFATS program determines the level of inspection staff and specialty training needed to assess cybersecurity at covered facilities, we examined documentation on the program's operations and organization, inspector and analyst performance management, cybersecurity training materials, and the program's training plans and evaluation forms. We also reviewed information on the cybersecurity codes that DHS assigned to CFATS program positions.[16] We interviewed CFATS and Cybersecurity and Infrastructure Security Agency human resource officials to obtain more information about the program's workforce processes and training efforts. We assessed the CFATS program's cybersecurity-related workforce plans and processes against our key practices in human capital management as well as DHS's internal guidance on workforce planning.[17] We also assessed the program's cybersecurity training efforts against our guide for assessing training and development efforts in the federal government.[18] The guide describes the four components of the training and development process: (1) Planning/Front-end Analysis, (2) Design/Development, (3) Implementation, and (4) Evaluation. Each component includes multiple questions to consider when assessing each of the four components, along with elements related to each question,

[16]DHS components are required to identify, code, and track their cybersecurity workforce in accordance with the Homeland Security Cybersecurity Workforce Assessment Act and Federal Cybersecurity Workforce Assessment Act of 2015, and guidance from the Office of Personnel Management. See Pub. L. No. 113-277, § 4, 128 Stat. 2995, 3008 (2014); Pub. L. No. 114-113, div. N, tit. III, § 303, 129 Stat. 2242, 2975. Specifically, DHS must designate work roles and associated codes for federal civilian positions performing information technology, cybersecurity, and other cyber-related functions. The cybersecurity codes align to the National Institute of Standards and Technology's National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.

[17]GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: March 2002).

[18]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004).

such as what measures the agency uses in assessing training and development efforts toward individual mastery and achieving agency goals. We used the following scale to evaluate the CFATS program's cybersecurity training efforts against the key practices that we identified from each of the four framework components and their respective questions.

- Generally addressed—program training materials and related documents and interviews with CFATS officials demonstrated that the CFATS program addressed most key practices.
- Partially addressed—program training materials and related documents and interviews with CFATS officials demonstrated that the CFATS program addressed some key practices.
- Not addressed—program training materials and related documents and interviews with CFATS officials did not demonstrate that the CFATS program addressed any of the key practices.

We conducted this performance audit from June 2019 to May 2020 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

Facilities Regulated by CFATS

As of February 2020, an estimated 3,300 facilities were designated as CFATS-covered facilities and subject to the CFATS regulations. These facilities possess any of the more than 300 chemicals of interest (COI), such as ammonia and chlorine, in quantities that meet or exceed a threshold quantity and concentration. The facilities also cross many industries, including, but not limited to, chemical manufacturing, storage, and distribution; energy and utilities; agriculture and food; explosives; pulp and paper; electronics; plastics; universities and laboratories; paint and coating; health care and pharmaceuticals; and metal production and finishing. COIs are categorized under three main security threats: release,

theft or diversion, and sabotage.[19] Release covers any toxic, flammable, or explosive chemicals or materials that can be released at a facility and potentially cause harm to the surrounding environment and population. Theft or diversion covers any chemicals or materials that, if stolen or diverted, can be converted into weapons using simple chemistry, equipment, or techniques. Sabotage covers chemicals or materials that can be mixed with readily available materials, such as water, to create significant adverse consequences for human life or health.

Cyber-Related Threats to the Chemical Sector

Information technology is a critical component of day-to-day chemical facility operations, including business systems and process control systems. While companies in the chemical sector have increasingly sought to gain efficiencies by connecting their physical security, information, and process control systems, the convergence between systems is a major challenge because it creates opportunities for potential cyber adversaries to access these systems.[20] In addition, process control systems are changing in ways that offer advantages to system operators but also make them more vulnerable to cyberattacks. In particular, proprietary devices in these systems are being replaced by cheaper and more widely available devices that use traditional networking protocols—including those that support remote access. Remote access capabilities in the devices can make them easier to maintain. Further, process control systems are being designed and implemented using traditional computer and operating systems, which allow them to be more easily connected to corporate business systems that support the sale, transfer, or distribution of chemicals. For example, malicious nation-state actors used spear phishing emails to deploy malware on business information technology (IT) networks in the 2015 attack on Ukrainian electricity utilities. After gaining initial access to the business IT networks, the attackers reportedly used a variety of techniques to access the industrial control system networks of the utilities.

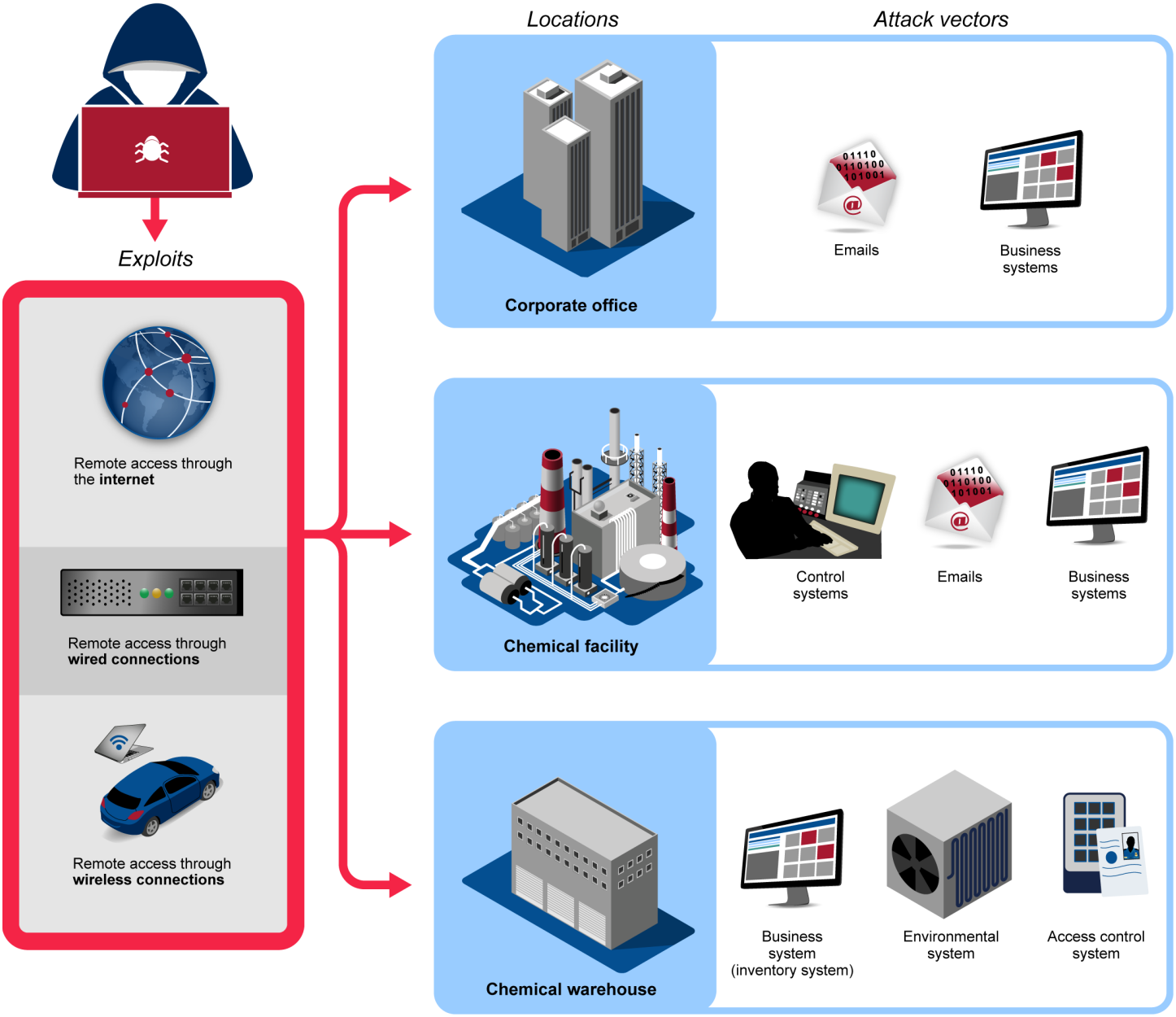
There are several types of risks to chemical facility information and process control systems, including ineffective protection of cyber assets, intentional or adversarial threats, or cyber threat adversaries.

[19]Appendix A of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 C.F.R. pt. 27) lists more than 300 chemicals of interest (COI), and their respective screening threshold quantities, which are categorized under the three main security issues listed above.

[20]GAO, *DHS Risk Assessments Inform Owners and Operator Protection Efforts and Departmental Strategic Planning*, GAO 18-62 (Washington, D.C.: October 2017).

- **Ineffective protection of cyber assets** can increase the likelihood of security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety. Unintentional or nonadversarial threat sources may include failures in equipment or software due to aging; resource depletion; and errors made by end users. They also include natural disasters and failures of the critical infrastructure on which the organization depends but that are outside the control of the organization.
- **Intentional or adversarial threats** may include corrupt employees, criminal groups, terrorists, and nations that seek to leverage the organization's dependence on cyber resources (i.e., information in electronic form, information and communication technologies, and communications and information-handling capabilities provided by those technologies). These threat adversaries vary in terms of their capabilities; willingness to act; and motives, which can include seeking monetary gain or seeking an economic, political, or military advantage.
- **Cyber threat adversaries** can make use of various techniques, tactics, practices—or exploits—to adversely affect an organization's computers, software, or networks or to intercept or steal valuable or sensitive information. These exploits are carried out through various conduits, including websites, email, wireless and cellular communications, internet protocols, portable media, and social media. In addition, adversaries can leverage common computer software programs, such as Adobe Acrobat and Microsoft Office, to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program. Further, cyber threat adversaries could infiltrate an information and process control system via the internet or other communication pathway to potentially disrupt its services and cause spills, releases, explosions, or fires. Moreover, process control systems, which were once largely isolated from the internet and the organization's information technology systems, are increasingly connected in modern chemical facilities, allowing cyberattacks to originate in business systems and migrate to operational systems. See figure 1 for potential cyber threats to CFATS-covered facilities.

Figure 1: Potential Cyber-Related Threats to Chemical Facilities



Source: GAO analysis of potential cybersecurity threats to chemical facilities. | GAO-20-453

Reports of successfully executed cyber exploits and known cyber-related threats illustrate the effects that these exploits can have on information and process control systems. In 2018, malicious nation-state actors used spear-phishing and other similar approaches against organizations to gain access to their networks and business systems, conduct reconnaissance, and collect and manipulate information about their industrial control system.[21] A malicious actor that gains access to information systems connected to a process control system could potentially gain access to the process control system. With this access, the actor could cause a loss of service or physical destruction by changing sensor settings or by manipulating the messages communicated to the process control system and causing controllers to make inappropriate changes.

CFATS Regulation and Guidance

Protecting against cyber-based attacks—such as cyber intrusions, malware attacks, and viruses—is a component of how the CFATS program assesses and helps to mitigate overall risk to covered chemical facilities. The CFATS program has developed guidance to help covered facilities effectively secure physical security, information, and process control systems from attack or manipulation, which typically includes a combination of policies and practices, such as access control policies and theft deterrence strategies.

The Department of Homeland Security Appropriations Act, 2007, required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities.[22] DHS enumerated 18 risk-based

[21]"Spear-phishing" involves sending official-looking emails to specific individuals to insert harmful software programs (malware) into protected computer systems; gain unauthorized access to proprietary business information; or access confidential data, such as passwords, Social Security numbers, and private account numbers. Federal Bureau of Investigation and National Cybersecurity and Communication Integration Center, *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*, TA18-106A (Washington, D.C.: Apr. 20, 2018 (revised)). DHS's National Cybersecurity and Communication Integration Center and the Federal Bureau of Investigation characterized the intrusions as a multistage intrusion campaign by identified nation-state actors on U.S. government entities, private-sector organizations, critical infrastructure providers, and the internet service providers supporting these entities. According to the agencies, the campaign targeted a number of legacy or weak protocols and service ports associated with network administration activities. The cyber actors used these weaknesses, among other things, to harvest login credentials and masquerade as privileged users. After obtaining access, the actors conducted network reconnaissance, manipulated industrial control systems and SCADA sensor messages, and created dangerous configurations that could have led to a loss of service or physical destruction.

[22]Pub. L. No. 109-295, § 550, 120 Stat.1335, 1388-89 (2006).

performance standards or performance standards that chemical facilities must meet to comply with CFATS, one of which is for cybersecurity. In addition, DHS produced the CFATS guidance in May 2009 to (1) assist covered facilities in selecting and implementing appropriate protective measures and practices and (2) help DHS personnel consistently evaluate measures and practices used by covered facilities.[23] The CFATS guidance is one of several documents used by DHS personnel to evaluate measures and practices used by covered facilities. Other documents used by DHS personnel include, among others, the Inspection Handbook, Cyber Inspection Handbook, Cyber Inspection Standard Operating Procedures, and Site Security Plan/Security Vulnerability Assessment Standard Operating Procedures.

Regarding the cybersecurity standard, the guidance provides a strategy for securing a facility's information and process control systems from attack or manipulation that typically includes a combination of policies and practices in several categories.[24] For example, the category of access control involves, among other practices, employing the "least privilege" concept (i.e., granting people only as much access as they need to perform their assigned job functions and no more) to cyber systems. The CFATS guidance provides additional details regarding these categories that can be used as aids by both covered facilities and inspectors.

To meet these performance standards, covered facilities may choose whatever security program or process they deem appropriate so long as the CFATS program determines that the facilities achieve the requisite level of performance in each applicable area.

CFATS Inspection Process

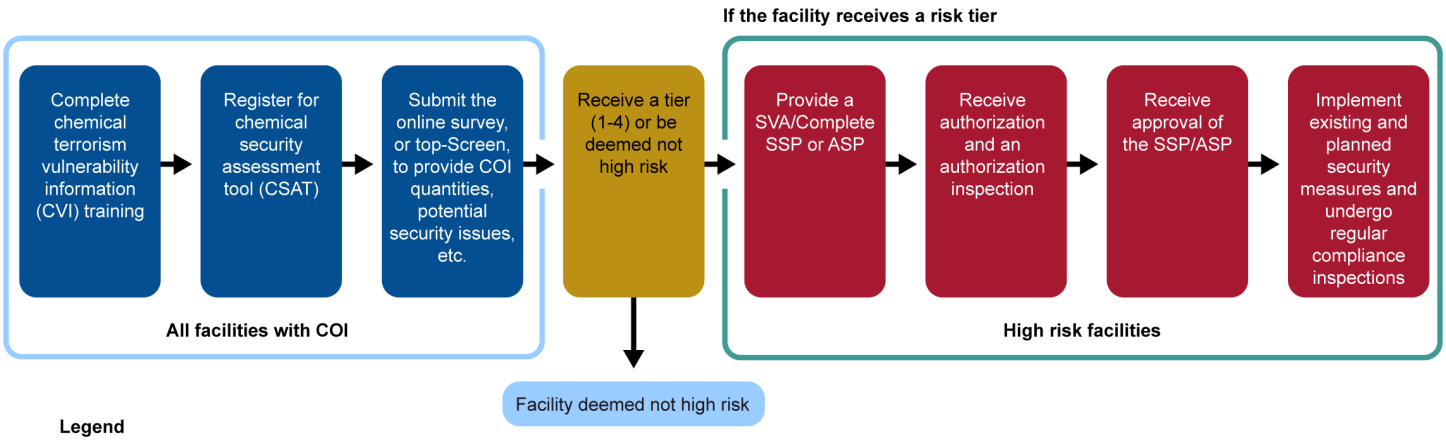
The CFATS inspection process includes several process stages, including reviewing security plans, conducting authorization inspections, approving security plans, and conducting compliance inspections. As of July 2019, CFATS had 136 inspectors to perform inspections in the field and two cyber analysts to provide support from headquarters.

See figure 2 for a depiction of the process stages.

[23]Department of Homeland Security, *Risk-Based Performance Standards Guidance, Chemical Facility Anti-Terrorism Standards* (May 2009).

[24]These categories include (1) security policy, (2) access control, (3) personnel security, (4) awareness and training, (5) monitoring and incident response, (6) disaster recovery and business continuity, (7) system development and acquisition, (8) configuration management, and (9) audits.

Figure 2: Inspection Process for Chemical Facility Anti-Terrorism Standards (CFATS) Chemical Facilities



Source: Department of Homeland Security CFATS inspection documentation. | GAO-20-453

Note: Chemical facilities that the Department of Homeland Security identifies as chemical facilities of interest and determine to meet risk criteria are called CFATS-covered chemical facilities.

- **Chemical-Terrorism Vulnerability Training.** Facility employees must complete Chemical-Terrorism Vulnerability Information training. The training informs employees about what CFATS-related vulnerability information needs to be protected from disclosure and how to protect it.[25]
- **Chemical Security Assessment Tool**. The Chemical Security Assessment Tool is an online portal that houses CFATS-related applications. A facility must register for access to the Chemical Security Assessment Tool. Once a facility has received access to the tool, the facility will have access to CFATS-related applications such as the Top-Screen survey, Security Vulnerability Assessment, and Site Security Plan.
- **Top-Screen.** A facility must submit a Top-Screen within 60 calendar days of coming into possession of a threshold level of the COI, unless statutorily excluded from CFATS. The Top-Screen is an online survey that includes, but is not limited to, information regarding the facility,

[25]Chemical-Terrorism Vulnerability Information is a designation used to protect information developed under the CFATS regulation (6 C.F.R. pt. 27) that relates to vulnerabilities of high-risk chemical facilities that manufacture, use, store, or otherwise possess certain explosives, reactive, flammable, or toxic chemicals of interests, to terrorist attacks. Only authorized users (or those that have received the training) with a need to know can have access to the information.

COI and COI quantities, storage conditions, and potential security issues.

- **Risk Tier.** The Infrastructure Security Compliance Division reviews the Top-Screen data to identify the facility's specific level of risk, and if it determines the facility is high-risk, assigns the facility to one of four tiers, with Tier 1 representing the highest risk and Tier 4 being the lowest. The tiering methodology takes into account three elements of risk in a facility's high-risk determination—(1) vulnerability, (2) consequences, and (3) threat. A facility not designated as high-risk is not subject to the additional requirements under the CFATS regulation.
- **Security Vulnerability Assessment and Site Security Plan**. When a facility receives a high-risk tier determination, the facility must complete and submit a Security Vulnerability Assessment and one of two types of security plans—Site Security Plan or an alternative security program—which describes the existing and planned security measures to be implemented in order to be in compliance with the applicable performance standards, including the cybersecurity standard.[26] The facility has 120 days from the date of written notification from DHS to submit the Security Vulnerability Assessment and security plan.
- **Authorization.** Once a facility submits a security plan, CFATS analysts review the security measures proposed by the facility. Analysts may provide additional suggestions that a facility may consider incorporating in order to ensure that they are meeting all applicable performance standards. After the CFATS program performs the initial security plan review, it sends a letter of authorization to the facility. Next, an authorization inspection is scheduled by the inspection team with the facility.
- **Authorization Inspection.** The purpose of the authorization inspection is to evaluate in person the accuracy of the facility's characteristics and the appropriateness of the security measures as documented in the facility's authorized security plan. The inspection team will evaluate the security measures through direct observation, document review, and interviews. Additionally, the inspection team will

[26]A Site Security Plan allows a facility to describe existing or planned security measures tailored to the risk level and unique considerations of the facility. An alternative security program allows a facility to develop its own template document for addressing CFATS requirements. An alternative security plan must describe how the facility's security measures will meet or exceed each performance standard and should appropriately address the tier and security concerns of the facility.

verify the facility's COI inventory against the latest submitted Top-Screen data. The inspection team works with the facility to review and revise the facility's submitted security plan in order to ensure that the facility meets the requirements of the applicable performance standards. If the inspection team determines a facility is not in compliance with its authorized security plan, the CFATS program may generate a notice to resolve the identified deficiencies at the facility. The facility must address the deficiencies and resubmit its security plan by a specified date. If the deficiencies cannot be resolved, DHS has the authority to pursue appropriate enforcement action, which could lead to the imposition of civil penalties.

- **Approval of Site Security Plan.** Once CFATS officials review and approve a facility's security plan, the department issues a letter of approval to the facility, and the facility must implement any existing and planned measures. For example, a planned measure for cybersecurity may include providing annual cybersecurity training and changing passwords. Inspectors verify that the planned measures are in place during subsequent compliance inspections.
- **Compliance Inspections.** After a facility's security plan is approved, the facility enters into the compliance inspection cycle. According to agency officials, the CFATS program will generally conduct the first compliance inspection within 12 to 18 months following the security plan approval. The compliance inspection is designed to confirm that the facility continues to implement its approved security plan and any associated planned measures that the facility agreed to implement as described in its approved security plan. If they find significant changes to existing planned measures, the inspectors assess the need for follow-up technical consultations or changes to the security plan, if necessary. Additionally, if the inspection teams finds that the facility is not in compliance with its approved Site Security Plan, the CFATS program may generate a notice to resolve identified infractions. The facility must resolve the identified infraction by a specified date or it may be subject to civil penalties.

As of July 2019, the CFATS program had a total of 147 inspector full-time equivalents (FTEs) (136 actual) across the program's 10 regional branches, based on our review of the Infrastructure Security Compliance Division's organization chart.[27] The program's Compliance Branch had 12 analyst FTEs (nine actual) in the branch's standardization and evaluation section, who are to be responsible for reviewing facilities' security plans and inspection reports submitted by the program's regional branches,

[27]This total comprises inspectors, supervisory inspectors, and senior inspectors.

among other duties, based on our review of the division's organization chart and interviews with CFATS officials.[28] This included three expert cyber analyst FTEs (two actual).

Cybersecurity Is Included in the CFATS Inspection Process; however, CFATS Guidance Is More Than 10 Years Old

The CFATS program evaluates cybersecurity during several stages in the inspection process. However, the CFATS program has not reviewed or updated its guidance for cybersecurity and other risks in more than 10 years.

Cybersecurity Considerations Are Included as Part of the Overall CFATS Inspection Process

Cybersecurity is considered during several stages of the CFATS inspection process—security plan approval, authorization inspections, and compliance inspections.

Security plan approval

During security plan approval, the cyber portion of the Site Security Plan is reviewed by cyber analysts at the CFATS program office in Infrastructure Security Compliance Division's headquarters. The cyber analysts will highlight any areas of concern and may offer additional points of consideration regarding a facility's cybersecurity measures. At this stage, the facility is assigned an initial cyber integration level—minimal, partial, or significant—which describes a facility's reliance on network-connected systems as it relates to the COI, according to the program's *Cyber Inspection Handbook.* The cyber integration level is an internal designation used to ensure that appropriately trained inspectors are present at an inspection and helps to guide inspectors' review of a facility's information and process control systems during an inspection. As of February 2020, CFATS officials estimate that 76 percent of covered facilities have been designated as minimal, 20 percent as partial, and 4 percent as significant.

[28]This total comprises analysts, specialists, and supervisory analysts.

- **Minimal.** A facility is designated as minimal if it has minimally integrated or minimally applied cyber systems into its security processes or control of its COI, according to the *Cyber Inspection Handbook.* This category of facility may be inspected by any inspector. For approval of a minimal integration facility, the facility should demonstrate the use of cybersecurity policies and procedures, access control, password management, physical security to cyber assets and media, incident reporting, and cybersecurity training.
- **Partial.** A facility is designated as partial if it has partially integrated or partially applied cyber systems into its security processes or control of the COI. This category requires an inspector who has additional training in cybersecurity or a headquarter-based cyber analyst to conduct the review. For approval of a partial integration facility, in addition to the minimal integration requirements above, the facility should use the following security measures: implement recurring audits; have documented business needs, system architecture, evaluation of vulnerabilities, and system boundaries and a cyber-incident response system; and have robust access control and password management protocols.
- **Significant.** A facility is designated as significant if it has completely integrated or significantly applied cyber systems into its security processes or control of the COI. This category requires additional cyber knowledge from a CFATS cyber analyst to conduct the inspection. For approval of a significant integration facility, in addition to the partial integration requirements identified above, the facility should use the following security measures: cybersecurity lifecycle integration, network monitoring, remote access restrictions (where applicable), back-up power, continuity of operations plans, information technology contingency plans, and disaster recovery plans.

Authorization Inspections

As described earlier, authorization inspections are intended to evaluate and ensure the facility is implementing the security measures as documented in the facility's approved security plan, including cybersecurity measures. The CFATS program uses the cyber integration levels—minimal, partial, or significant—to determine the necessary team to perform the cybersecurity portion of an inspection. For significantly integrated facilities, cyber analysts at headquarters may be consulted prior to or during the inspection. Additionally, if needed, cyber analysts may be requested to accompany an inspector during an inspection.

Compliance Inspections

As previously mentioned, during compliance inspections, the CFATS program confirms that the facility continues to implement its approved security plan and any associated planned measures that the facility

agreed to implement as described in its approved security plan. The inspection team will use document review, interviews, and observations to verify the facility's current cybersecurity measures and the status of any cybersecurity planned measures. For example, during two compliance inspections, we observed inspectors reviewing documents, such as policies and network maps, and interviewing facility personnel to determine the facility's progress on planned measures to be implemented. In addition, the inspectors compared the information in the facility's case file to the security measures implemented at the facility to ensure compliance with the cybersecurity standard. Further, we observed the inspectors touring the physical security and process control operations centers and the server rooms to determine if access controls were in place and interviewing operators about any system changes and security measures.

During the inspection process, officials confirmed the CFATS program does not conduct any type of vulnerability or penetration testing on a facility's network or systems to test its cybersecurity-related controls. In addition, the inspection team does not interact directly with a facility's network, systems, or cyber-related processes in any way because it may cause adverse effects on a facility's information systems, components, or day-to-day business or process operations. In lieu of such procedures, an inspector may request a functional demonstration. A functional demonstration is used to validate the proper functioning of cybersecurity controls. However, if the facility's personnel determine that a functional demonstration would violate a facility's policies or procedures, they can deny the inspector's request to perform it. In this case, the inspector can request additional documentation or information in lieu of the demonstration to verify that the security measure is in place.

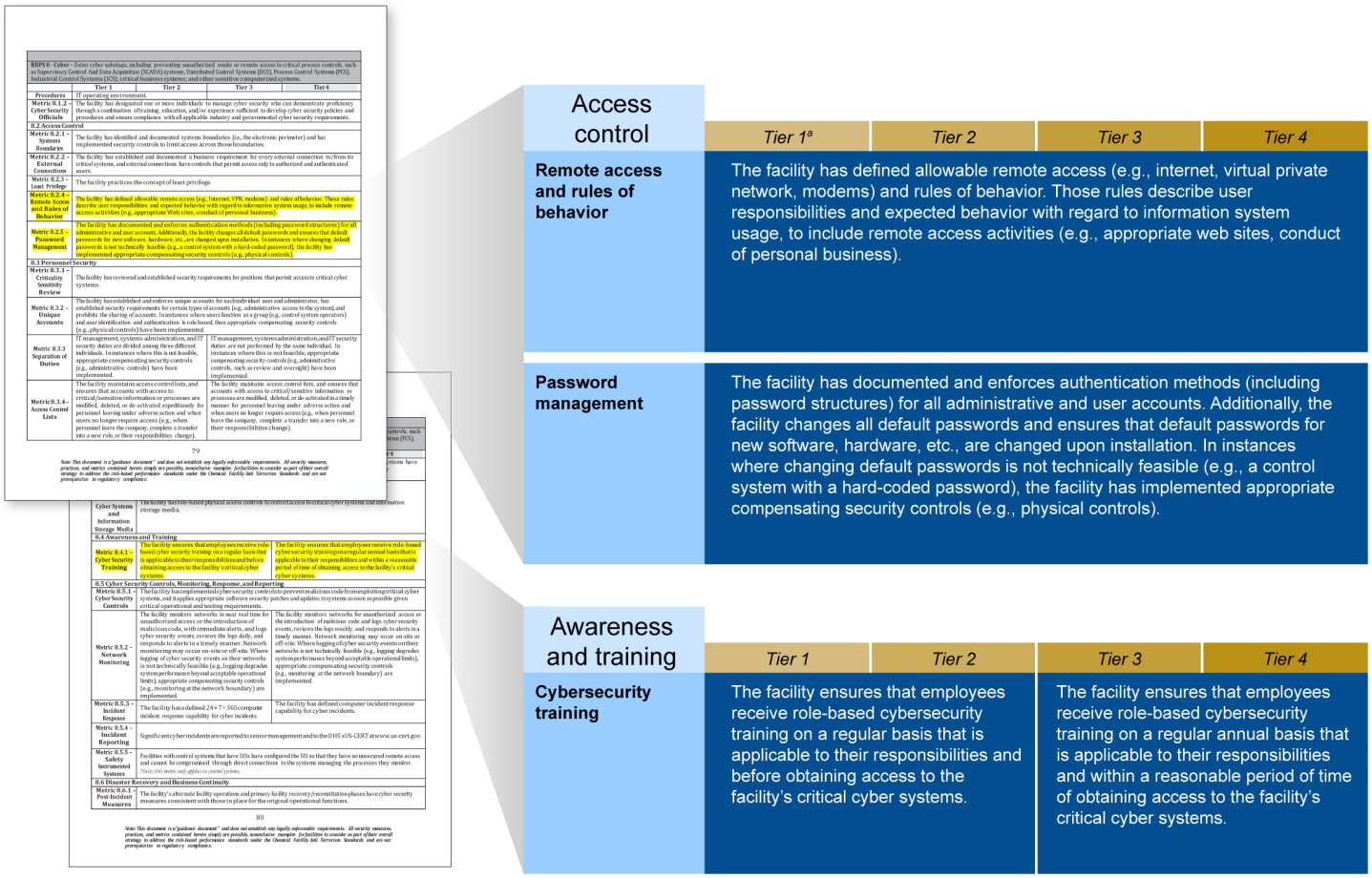
CFATS Performance Standard Guidance Has Not Been Reviewed or Updated in More Than 10 Years

The CFATS program has not reviewed or updated the guidance designed to help facilities comply with the cybersecurity and other performance standards for more than 10 years, despite the guidance itself acknowledging the importance of updating and revising it.

While the CFATS guidance does not prescribe specific actions covered facilities must take to meet the performance standards, it does offer examples of measures and practices that facilities may choose to consider as part of their strategy to meet the cybersecurity and other performance standards. For example, the CFATS guidance provides examples of various security measures and practices a facility may employ to reduce vulnerability and risks, including specific activities and targets a facility may seek to achieve that could allow it to be considered

compliant with the cybersecurity and other performance standards. The CFATS guidance states that cyber systems that a facility might consider critical could include, but are not limited to, those that monitor or control physical processes that contain a COI; contain business or personal data that could be exploited to steal, divert, or sabotage a COI; and other systems that manage physical processes that contain a COI. The guidance aims to help covered facilities identify security measures that could be incorporated into their security plans. Figure 3 highlights activities that facilities may consider implementing to meet the cybersecurity standard, according to the 2009 guidance.

Figure 3: Examples of Cybersecurity Practices in the Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards Guidance



Source: Department of Homeland Security, Risk-Based Performance Standards Guidance, May 2009. | GAO-20-453

[a]The CFATS program assigns high-risk facilities to one of four tiers with Tier 1 representing the highest risk and Tier 4 being the lowest.

Based on our interviews with industry associations, we found that the cybersecurity practices and activities within the guidance were useful tools for some covered facilities. Officials at three of the five chemical industry associations we interviewed stated that the guidance is helpful because it provides a baseline for covered facilities to achieve. However, officials from two associations stated that the guidance was no longer as relevant for their larger member companies, since those companies have more monetary and human resources for cybersecurity-related efforts, and have implemented other cybersecurity guidance and standards that meet or exceed the guidance provided by DHS.[29] Officials at one of the associations said that, due to the passage of time since its issuance, the larger corporations may no longer find the guidance as useful because their cybersecurity programs have matured beyond it. However, these same association officials also acknowledged that smaller companies with less sophisticated information and industrial control systems and with fewer resources likely find the DHS guidance more applicable and useful.

The CFATS *Risk-Based Performance Standards Guidance* asserts the importance of updating and revising guidance information, as needed, and states that the document is likely to be periodically updated to take into account any lessons learned throughout the CFATS implementation and new security approaches and measures that covered facilities may wish to consider implementing. In addition, CFATS program officials stated that reviewing the guidance to determine what updates may be needed could be helpful, given technological advancements such as cloud computing and the development of other, more recent cybersecurity practices and industry guidance, such as the NIST Cybersecurity Framework.[30] The CFATS guidance is also designed to serve as a resource for inspectors in their efforts to partner and advise covered

[29]During our interviews, associations referred to the National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Gaithersburg, M.D.: Feb. 12, 2014) and the Department of Homeland Security, *Chemical Sector Cybersecurity Framework Implementation Guidance*, which have been issued since the CFATS *Risk-Based Performance Standards Guidance* and may have applicability. In addition, the International Standard for Organization 27001, the Industrial Society of Automation Standard 99, and the American Chemistry Council Responsible Care Code were identified as being other standards used by the chemical industry.

[30]The NIST Cybersecurity Framework is a nationally recognized set of voluntary standards and procedures that critical infrastructure facilities may use to manage and assess their cybersecurity risks.

facilities of potential options to consider. CFATS officials stated that, as the program matured, they recognized the need to provide updated and supplemental guidance for inspectors to help improve inspector understanding on how to evaluate and implement CFATS security measures. However, CFATS program officials also acknowledged that the program does not have a documented process for reviewing and revising the guidance.

The CFATS program has issued multiple documents related to governance of the inspection process since the May 2009 issuance of the CFATS guidance, such as inspection standard operating procedures, handbooks, and other specific guidance relevant to cybersecurity.[31] However, these documents are not designed to assist facilities with identifying approaches to cybersecurity. In addition, DHS conducted two reviews related to the NIST Cybersecurity Framework and the CFATS program.

- In 2015, DHS worked with the Chemical Sector Coordinating Council and the sector's Government Coordinating Council to develop NIST Cybersecurity Framework implementation guidance specifically for Chemical Sector owners and operators, regardless of their size, cybersecurity risk, or level of cybersecurity sophistication.[32] The DHS's chemical industry implementation guidance mapped existing chemical sector cybersecurity materials, such as tools, standards, and approaches, including those related to CFATS, to the key categories of the NIST Cybersecurity Framework, such as access control, data security, awareness and training, and recovery planning.[33] The mapping identified several areas of potential gaps where CFATS material does not include a particular category of the NIST

[31]These documents include the program's cyber handbook, cyber standard operating procedure, and the post-inspection report, authorization inspection report, and compliance inspection report guidance.

[32]Sector Coordinating Councils are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. Government Coordinating Councils (GCCs) are formed as the government counterpart for each Sector Coordinating Council to enable interagency and cross-jurisdictional coordination. The GCC are comprised of representatives from across various levels of government (federal, state, local, or tribal), as appropriate to the operating landscape of each individual sector.

[33]Department of Homeland Security, *Chemical Sector Cybersecurity Framework Implementation Guidance,* 2015.

Cybersecurity Framework. For example, incorporating lessons learned into recovery processes is not addressed as it is in the NIST Cybersecurity Framework.

- In 2014, DHS conducted an analysis comparing metrics listed in CFATS guidance for the cybersecurity standard with the NIST Cybersecurity Framework in response to Executive Order 13636 on Improving Critical Infrastructure Cybersecurity.[34] While DHS determined that no significant gaps existed, the analysis did identify some items with the potential to strengthen the CFATS cybersecurity standard that may warrant future consideration. For example, it identified protecting removable media and requiring configuration change controls as subjects for consideration.

Standards for Internal Control in the Federal Government states that periodic review of policies, procedures, and related control activities should occur to determine their continued relevance and effectiveness in achieving identified objectives or addressing related risks. In addition, documentation of any changes made, such as changes to an entity's roles and responsibilities or in technology, should occur to ensure that such controls are clear over time as staff change within an organization.[35] However, despite the availability of recent guidance and other tools, the CFATS program does not have a process to routinely or periodically update its performance standards guidance that regulated chemical facilities and CFATS inspectors use to help implement the cybersecurity standard. Given the rapid changes in the current cybersecurity landscape, especially in relation to the increasing frequency and sophistication of cyberattacks against process control systems and evolving cyber threats overall, it is important that the CFATS program have a process to ensure that it is sharing current, timely, and relevant guidance with industry so that covered chemical facilities can plan accordingly and protect their critical cyber assets from attack.

[34]Cybersecurity and Infrastructure Security Agency (CISA), Executive Order 13636-Improving Critical Infrastructure Cybersecurity Section 10 (b) Report on the Department of Homeland Security's Chemical Facilities Anti-Terrorism Standards, in the CISA Publications Library, accessed April 13, 2020, https://www.cisa.gov/publication/eo-13636-improving-ci-cybersecurity. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[35]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C: September 2014).

CFATS Provides Cybersecurity Training for Inspectors but Does Not Fully Incorporate Key Training and Workforce Planning Practices to Address Cybersecurity Needs

The CFATS program has taken several steps to develop and provide cybersecurity training for inspectors, but it does not systematically collect performance data for this training and does not have a process to evaluate its effectiveness. Additionally, the program does not incorporate cybersecurity needs into aspects of its workforce planning processes and does not have a process to track program-related cybersecurity data that could aid in workforce planning efforts.

CFATS Provides a Range of Cybersecurity Training for Inspectors but Does Not Collect Training Data or Evaluate Its Effectiveness as Recommended by Key Training Practices

In 2004, GAO developed a framework designed to serve as a flexible and useful guide in assessing how agencies plan, design, implement, and evaluate effective training and development programs that contribute to improved organizational performance and enhanced employee skills and competencies.[36] The framework summarizes attributes of effective training and development programs and is intended to help managers assess an agency's training and development efforts and make it easier to determine what, where, and how improvements may be implemented.[37] We found that the CFATS program generally addressed one of the four framework components for developing effective training and development programs and partially addressed the other three components. Table 1 provides an overview of our assessment of how the CFATS program addressed the key practices we identified from each of the four framework components and their respective questions.

[36]GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004). The framework focuses primarily on training and development rather than other important methods of learning within an organization, such as knowledge management.

[37]Taken as a whole, the training and development process can be segmented into four broad, interrelated components: (1) Planning/Front-end Analysis, (2) Design/Development, (3) Implementation, and (4) Evaluation. Each component comprises a series of questions to consider in assessing a training and development program. For the purposes of our review, we identified and summarized the four key practices based on each of the components and their respective questions. Although we discuss these practices separately, it is important to recognize that these practices are not mutually exclusive and encompass subcomponents that may blend with one another. For example, evaluation blends with the others, as it should occur continuously throughout the training and development process.

Table 1: GAO Assessment of Chemical Facility Anti-Terrorism Standards (CFATS) Training Efforts Against Key Training Practices

Key practices	Assessment
Identify training needs and measures to assess how training will contribute to program results *(Planning/Front-end Analysis).* Questions assessed include: • Does the agency have training goals and related performance measures that are consistent with its overall mission, goals, and culture? • How does the agency determine the skills and competencies its workforce needs to achieve current, emerging, and future agency goals and missions and identify gaps, including those that training and development strategies can help address? • What measures does the agency use in assessing the contributions that training and development efforts make toward individual mastery of learning and achieving agency goals?	Partially addressed
Design training program to address goals or gaps *(Design/Development).* Questions assessed include: • How is the design of the training or development program integrated with other strategies to improve performance and meet emerging demands, such as changing work processes, measuring performance, and providing performance incentives? • Does the agency use the most appropriate mix of centralized and decentralized approaches for its training and development programs? • How does the agency compare the merits of different delivery mechanisms (such as classroom or computer-based training) and determine what mix of mechanisms to use to ensure efficient and cost-effective delivery?	Generally addressed
Implement training and collect performance data *(Implementation).* Questions assessed include: • Are agency managers responsible for reinforcing new behaviors, providing useful tools, and identifying and removing barriers to help employees implement learned behaviors on the job? • How does the agency select employees (or provide the opportunity for employees to self-select) to participate in training and development efforts? • Does the agency collect data during implementation to ensure feedback on its training and development programs?	Partially addressed

Key practices	Assessment
Evaluate the effectiveness of training *(Evaluation)*. Questions assessed include: • To what extent does the agency systematically plan for and evaluate the effectiveness of its training and development efforts? • How does the agency incorporate evaluation feedback into the planning, design, and implementation of its training and development efforts? • Does the agency incorporate different perspectives (including those of line managers and staff; customers; and experts in areas such as financial, information, and human capital management) in assessing the impact of training on performance?	Partially addressed

Source: GAO analysis of CFATS training documents and interviews with CFATS officials. | GAO-04-546G and GAO-20-453

Note: We assigned one of the following categories to describe how the CFATS program's cybersecurity training efforts addressed several key practices in developing training and development programs:

Generally addressed—Program training materials and related documents and interviews with CFATS officials demonstrated that the CFATS program addressed most key practices.

Partially addressed—Program training materials and related documents and interviews with CFATS officials demonstrated that the CFATS program addressed some key practices.

Not addressed—Program training materials and related documents and interviews with CFATS officials did not demonstrate that the CFATS program addressed any of the key practices.

Identify Training Needs and Measures to Assess How Training Will Contribute to Program Results

The CFATS program partially addressed the key practice of identifying training needs and measures to assess how training will contribute to program results. We found that the CFATS program took steps to identify its cybersecurity training needs, but it has not identified measures to assess how training will contribute to program results. According to key practices, front-end analysis can help ensure that training and development efforts are not initiated in an ad hoc, uncoordinated manner but rather are strategically focused on improving performance toward the agency's goals and are put forward with the agency's organizational culture firmly in mind.[38] As part of this process, an agency should consider the viewpoints of managers and other stakeholders in addressing its training efforts and determine the skills and competencies needed to meet current and future challenges and assess related gaps. It should also set forth measures to assess how training efforts will contribute to achieving agency results, such as targets and goals that establish how training strategies are expected to contribute to improved program results.

The CFATS program has taken steps to identify its cybersecurity training needs for inspectors and overcome related challenges in keeping this training up-to-date. For example, the program's headquarters and

[38]GAO-04-546G.

regional staff identify cybersecurity and other training needs for inspectors on an ongoing basis and report these needs to the program's management for further exploration, according to a CFATS official. Additionally, the Infrastructure Security Compliance Division aims to review the division's training curriculum every 2 to 3 years. A CFATS official at headquarters told us the program recognized that improvements to cybersecurity training are an ongoing effort due to the fast-paced and complex nature of cybersecurity-related threats and vulnerabilities. In addition, CFATS officials told us that one of the biggest challenges related to the program's cybersecurity efforts is keeping the program's training up-to-date in the face of frequent technological changes and advances. A CFATS official stated that, in 2019, the program reevaluated its cybersecurity training and worked with a contractor to develop an updated training module aimed at addressing inspector training requirements and needs. Also in 2019, the Infrastructure Security Compliance Division conducted a separate survey and analysis of training gaps for personnel as part of a division-wide training improvement project and identified gaps in CFATS inspector and analyst cybersecurity training, according to division training and planning documents.

Although the CFATS program has undertaken efforts to determine its cybersecurity training needs, the program has not developed measures to assess how training will contribute to program results. Such measures could include targets for enhanced inspector or program performance related to cybersecurity, based on our analysis of key training practices. The program has not developed such measures because cybersecurity training is difficult to isolate from the other performance standards, based on our review of an interview with a CFATS official. Specifically, the official told us that the program prioritizes all of its 18 performance standards at the same level, and the cybersecurity standard extends to other standards, such as conducting background checks on personnel, because of the cross-cutting nature of cybersecurity. As such, the program's training is cross-cutting to contain elements of all performance standards that inspectors are required to evaluate at covered facilities. However, trainings that include cybersecurity can be identified and assessed for contributions to program cybersecurity goals, but the program has not done so to date. For example, two of the four trainings the program provided to inspectors in 2018 that included a cybersecurity component did not include learning objectives as part of the training

module, based on our review of program training materials.[39] Learning objectives should be used to help define training goals that measure how training is contributing to organizational results, according to key practices.[40] As a result, the program is unable to determine whether the resources it has allocated for cybersecurity training is helping to improve inspectors' cybersecurity skills and competencies.

Design Training Program to Address Goals or Gaps

The CFATS program generally addressed the key practice of designing a training program to address goals or gaps by designing cybersecurity training for inspectors. When designing training programs, agencies should consider using a variety of instructional approaches to achieve learning, limiting overlap and duplication and ensuring the delivery of an integrated message through either a centralized or decentralized approach, and integrating training with other strategies to meet emerging demands.[41] Determining the optimal approaches or strategies that address agency goals and skills gaps can help agencies design effective and efficient training programs that enhance performance.

The CFATS program provided a mix of formal, informal, and on-the-job training in an effort to equip inspectors with the skills needed to conduct the cybersecurity portion of inspections, based on our review of training materials and interviews with CFATS officials. The program uses a centralized approach to training, in which mostly headquarters officials, including the program's cyber analysts, prioritize, design, and organize cybersecurity training for inspectors, according to an Infrastructure Security Compliance Division training document and CFATS officials. The program also provides webinars and refresher training that addresses cybersecurity topics. Inspectors and headquarters-based cyber analysts also have the option of taking additional DHS-provided cybersecurity training. For example, inspectors can take training via the division's online learning tool and DHS's Industrial Control Systems Cyber Emergency Response Team virtual learning portal. Inspectors and cyber analysts may also request to take external training or work toward obtaining

[39]In 2018, the CFATS program provided two inspection guidance webinars and one refresher training that, among other topics, included guidance on determining cyber integration levels at covered chemical facilities. Also that year, the program provided a refresher training on its cybersecurity standard and guidance.

[40]A learning objective is a statement of the desired changes that the specific training and development program is intended to produce in the target population's skills, knowledge, abilities, or behaviors.

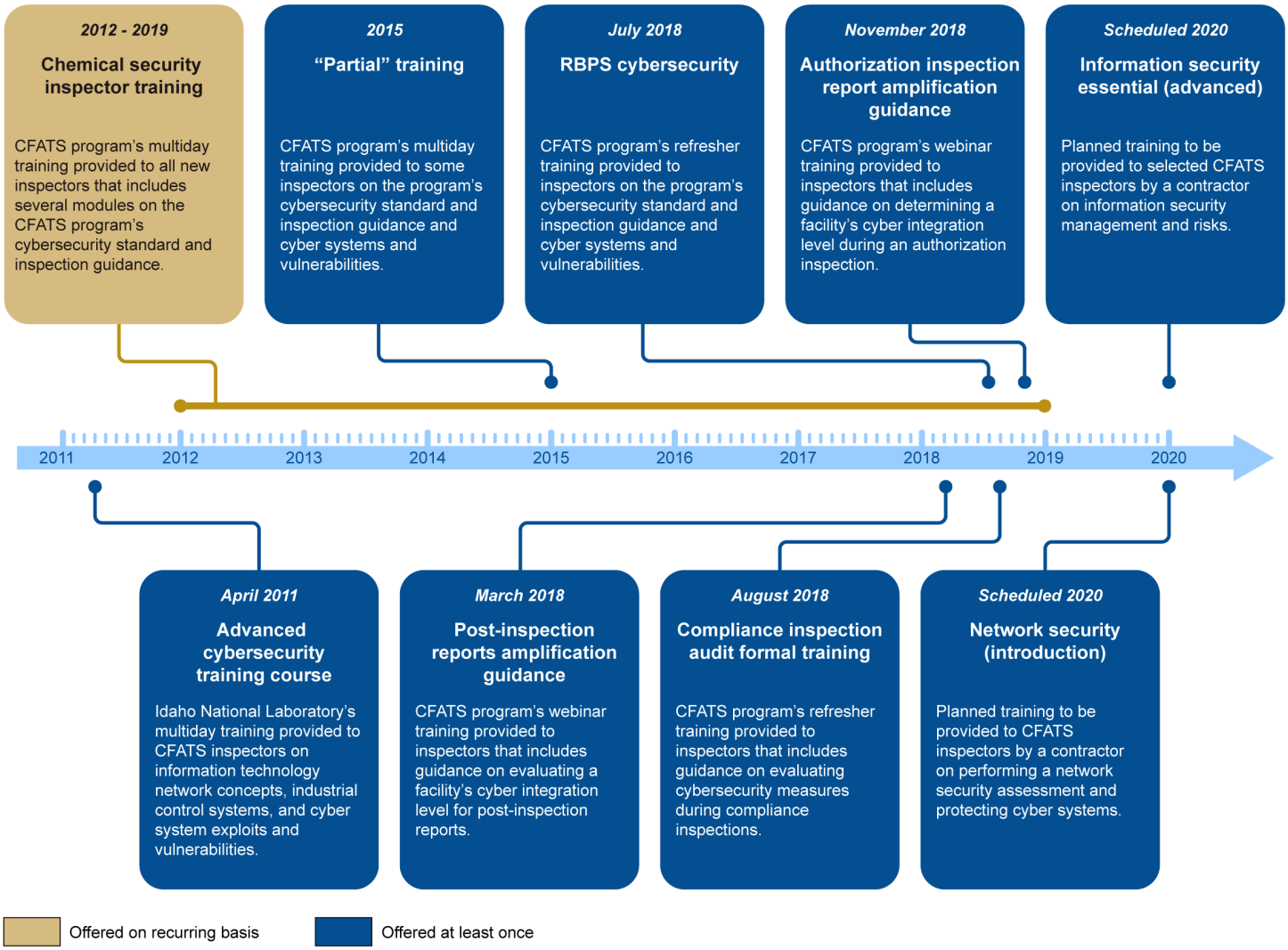
[41]GAO-04-546G.

professional cyber certifications.[42] CFATS officials told us that inspectors and cyber analysts have attended a variety of cybersecurity-related external training courses and conferences to enhance cybersecurity expertise, such as courses on cybersecurity planning and critical security controls.

As the CFATS program's approach to conducting the cybersecurity portion of inspections has changed over time, the program has adjusted its training accordingly (see fig. 4). For example, the program began offering cybersecurity training as part of its onboarding training for inspectors in 2012. According to CFATS officials, the program recognized the need to provide more advanced cybersecurity training and, in 2015, offered the "partial" training course—which was the only in-house course the program offered that specifically addressed cybersecurity. As previously mentioned, the program is working with a contractor to develop two new cybersecurity courses—introductory and advanced—aimed at addressing gaps in inspectors' cybersecurity skills that the program identified, such as practical knowledge on the fundamentals of computer hardware, operating system, networks, industrial control systems, and information security concepts, according to program training documents.

[42]Some inspectors also have taken courses for cyber certification programs, such as the Certified Information Systems Security Professional and Certified Information Systems Auditor programs. These programs have several requirements for certification, such as the successful completion of an exam and a minimum number of years of related work experience, as well as a continuing professional education requirement to maintain the certification.

Figure 4: Chemical Facility Anti-Terrorism Standards (CFATS) Cybersecurity-Related Training, 2011-2020



Source: GAO analysis of CFATS training documents and materials. | GAO-20-453

Implement Training and Collect Performance Data

The CFATS program partially addressed the key practice of implementing training and collecting performance data by taking steps to support developing inspectors' and analysts' cybersecurity skills; however, the program does not systematically collect training performance data, such as the number of training participants, as specified in our key practices. Implementing a training program involves ensuring the effective and efficient delivery of training opportunities in an environment that supports learning and change, which gives agencies the opportunity to empower

employees and improve performance.[43] As part of this process, agencies should hold managers and employees accountable for supporting training efforts, ensure employee are selected for the appropriate training or have the option to self-select for additional training, and collect training performance data to assess progress made toward achieving results.

The CFATS program supports training and development goals related to cybersecurity for inspectors and analysts through several performance management processes, based on a review of sample inspector and analyst performance plan activities and goals and information from CFATS officials.[44] For example, one inspector's performance plan included a goal of enhancing cybersecurity knowledge, among other goals, and specified several activities the inspector could take to achieve the goal, such as participating in an internal or external training course pertaining to cybersecurity. Additionally, a supervisory inspector told us that inspectors are encouraged to add training courses of interest to them in their individual development plans.

A CFATS official at headquarters noted that supervisors review and approve external training requests based on budget and applicability to the job, and attendance is not guaranteed. For example, one inspector told us that he used his own funds to pay for an external course on cybersecurity for first responders, including travel expenses, because the program denied his training request. A supervisory inspector also said that inspectors are not required to take additional cybersecurity-related training or expected to have cybersecurity certifications. Similarly, cyber analysts may identify and request additional training in their individual development plans. However, none of the example performance plan activities and goals for cyber analysts or supervisory inspectors that CFATS officials provided us included a cybersecurity training component. In addition, a CFATS official told us that there were no training requirements related to industrial control systems for cyber analysts. Separately, a supervisory inspector told us that inspector performance plans contain a professional development component and that the

[43]GAO-04-546G.

[44]CFATS officials provided example performance plan activities and goals for inspectors, supervisory inspectors, cyber analysts, and supervisory cyber analysts. These examples are nongeneralizable to the performance plans of all of the program's inspectors and analysts.

program was working on adding a training component for fiscal year 2020.

The CFATS program currently offers additional cybersecurity training on an irregular and voluntary basis.[45] For example, the program offered additional cybersecurity-related training courses, refresher training, and webinars in 2011, 2015, and 2018 and has plans to offer two new courses in 2020. In addition, a CFATS official told us that the program offered the "partial" training course—the only in-house training course the program offered that specifically addressed cybersecurity—on a voluntary basis; approximately 61 percent (83 of 136) of inspectors completed the training, based on our review of the program's training and personnel documents.[46] A CFATS official at headquarters told us that the two new cybersecurity training courses—introductory and advanced—will also be offered on a voluntary basis for inspectors, and the advanced course will be offered on a limited basis. The official estimated that most, if not all, inspectors would take the new cybersecurity training because of the increased interest in the topic, and, to date, have not negotiated with the union to make these courses mandatory. However, regional officials provided differing perspectives on the level of interest inspectors had in taking additional cybersecurity training. For example, a regional official told us that none of the inspectors in his region have requested more training on cybersecurity, whereas an inspector from another region told us that he wanted to attend more cybersecurity-related training courses and conferences.

The CFATS program does not systematically collect or track delivery and performance data related to inspectors' cybersecurity training or information on inspectors' cybersecurity expertise, based on written responses from and interviews with CFATS officials. For example, CFATS officials were unable to provide information on which inspectors have taken cybersecurity-related training courses, webinars, or refreshers—with the exception of attendees for "partial" training—

[45]All newly hired inspectors take the Chemical Security Inspector training course, which includes several modules on the CFATS program's cybersecurity standard and inspection guidance.

[46]This percentage is based on the overall number of CFATS inspectors, supervisory inspectors, and senior inspectors as of July 2019.

because the records were dated and could not be located.[47] Regarding the "partial" training, CFATS officials compiled a list of attendees for the course by combining sign-in sheets and queries from inspectors who had attended the training based on our request rather than by maintaining a list of attendees. We found that CFATS officials' perspectives on how many inspectors completed the "partial" training varied across region and in the data provided. For example, a manager in Region 6 told us that all of the inspectors in their respective region attended the "partial" training. However, based on our analysis of the attendee list CFATS officials compiled, as of August 2019, 10 of the 18 inspectors in Region 6 completed the "partial" training.[48] CFATS officials also stated that any external training or professional certifications that an inspector may have received related to cybersecurity is not tracked and is available only in inspectors' personal files.

Our previous work on the federal government's cybersecurity workforce planning efforts found that DHS lacked the ability to view or easily produce information on the industry-recognized certifications held by their employees.[49] Similarly, we found during our audit work that the CFATS program was unable to easily produce complete information on the cybersecurity expertise of all the program's inspectors. For example, CFATS officials provided us examples of cybersecurity external training and professional certifications that inspectors received compiled from a query of selected inspectors rather than from existing personnel files. As a result, the program may not have sufficient or reliable information to accurately evaluate inspector cybersecurity skills and competencies or, as previously mentioned, how training is contributing to improved inspector or program performance.

Evaluate the Effectiveness of Training

The CFATS program partially addressed the key practice of evaluating the effectiveness of training by taking some steps to evaluate the effectiveness of its cybersecurity training, but it does not systematically

[47]CFATS officials provided an attendee list for a Personnel Surety refresher training course offered in July 2019. This training was primarily focused on the new personnel surety guidance for the CFATS program, and had a brief mention of cybersecurity, based on our review of program training materials. As a result, we excluded this training from the scope of our review.

[48]Inspector totals are based on the overall number of CFATS inspectors, supervisory inspectors, and senior inspectors in Region 6, as of July 2019.

[49]GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466 (Washington, D.C.: June 2019).

collect or track information that could be used to evaluate its effectiveness. Evaluating an agency's training program and demonstrating how these efforts help develop employees and improve agency performance can aid decision makers in managing scarce resources.[50] As part of this process, agencies need to collect credible information on how training programs affect organization performance, such as employee or stakeholder feedback on training efforts and impact of training on organizational results, and develop evaluation processes that assess the benefits of these efforts.

CFATS officials told us that they evaluate the effectiveness of cybersecurity training by observing inspections and conducting quality control reviews and audits of inspection reports. Specifically, in fiscal year 2019, the CFATS program implemented a new auditing process aimed at enhancing the accuracy and consistency of its operations, according to our review of program planning documents and an interview with a CFATS official. Headquarters-based cyber analysts are sent to the field to observe inspections, and program managers conduct quality control reviews of inspection reports. If a performance issue is identified, an inspector is assigned a mentor or must attend additional training or receive on-the-job training. Headquarters-based officials also request that regional managers share ideas and request assistance to ensure the consistency of CFATS inspections.

However, the program does not systematically collect or track information that could be used to evaluate the effectiveness of its cybersecurity-related training, such as feedback surveys or course evaluation forms, based on written responses and interviews with CFATS officials. For example, CFATS officials were unable to produce completed or example evaluation forms for most of program's training courses, webinars, or refreshers related to cybersecurity, and, in the case of the "partial" training, feedback surveys were not conducted. CFATS officials provided us example course evaluation forms for the inspector onboarding training course from fiscal year 2012. The forms included a section for participants to give feedback on the course's overall delivery and design and knowledge and skills acquired. CFATS officials told us that they were unable to provide course evaluation forms for other cybersecurity trainings because the records were dated and could not be located. As a result, the program may not be able to fully assess how training is

[50]GAO-04-546G.

improving inspectors' capability to conduct the cybersecurity portion of inspections.

CFATS inspectors provided varying perspectives on the effectiveness of the CFATS program's cybersecurity training. For example, one inspector stated that he felt that he did not have sufficient training to evaluate the implementation of the program's cybersecurity standard at covered chemical facilities, and he identified the lack of relevant cybersecurity training as one of the challenges facing the program related to cybersecurity. The inspector recommended that additional cybersecurity training should be provided. During a Senate Homeland Security and Governmental Affairs Committee roundtable in 2018, another inspector testified that the program's cybersecurity training did not provide inspectors with information on how to analyze, understand, and protect the cyber systems of covered chemical facilities.[51] In contrast, a supervisory inspector we interviewed stated that he believed that the inspectors in his region have the cybersecurity training needed to conduct the cybersecurity portion of inspections as required.

Since the CFATS program does not collect or track performance data for its cybersecurity training or identify measures to assess how its cybersecurity training is contributing to program results, it is unable to verify which inspectors have the skills and competencies needed to conduct the cybersecurity portion of inspections and whether its training is effective in improving inspector and program performance related to cybersecurity. This raises the risk that inspectors may not be effectively conducting these reviews and accurately assessing the cybersecurity posture of covered chemical facilities. By incorporating these leading practices into its latest cybersecurity training efforts, the CFATS program could better verify the cybersecurity expertise of its inspector workforce and whether the training is addressing cybersecurity needs and gaps in skills that the program and the Infrastructure Security Compliance Division have identified.

[51]Jesse LeGros, Jr., Vice President, Infrastructure Protection, AFGE National Local #918, *Roundtable – Examining the Chemical Facility Anti-Terrorism Standards Program*, testimony before the Senate Committee on Homeland Security and Governmental Affairs, 115th Cong., 2nd sess., June 12, 2018.

CFATS Does Not Address Cybersecurity Needs in Workforce Planning Processes

The CFATS program does not evaluate or address its needs related to cybersecurity in several of its workforce planning processes. CFATS officials told us that their workforce planning decisions are guided by broad program goals outlined in the Infrastructure Security Compliance Division's annual operating plan and cybersecurity needs are not evaluated separately from these goals.[52] In addition, DHS's Cybersecurity Workforce Strategy Fiscal Years 2019-2023 outlines agency goals and strategies for its cyber workforce, such as identifying workforce needs; recruiting highly qualified and diverse cybersecurity talent; building cybersecurity capabilities through training and professional development; and leveraging government-wide flexibilities for recruiting, hiring, training, and retention efforts. However, our review of the Infrastructure Security Compliance Division's fiscal year 2019 operating plan found that none of the division's primary goals, core CFATS mission activities, or projects are directly related to the CFATS program's cybersecurity standard and guidance or its inspection efforts.[53]

According to CFATS officials, the program has no formal process or tool to evaluate its workforce needs, including those related to cybersecurity. Workforce planning decisions are made at division-level team meetings, where headquarters and regional managers identify, review, and determine staffing needs and resources based on program goals. In general, the program prioritizes staffing needs based on the inspector-to-facility ratio in the program's 10 regions.[54] As of July 2019, the CFATS program had FTE vacancies for one cyber analyst at headquarters and 11 inspectors across six of its 10 regional branches, based on our review

[52]The Infrastructure Security Compliance Division's fiscal year 2019 Annual Operating Plan describes the division's operating structure as well as the goals, objectives, activities, and projects associated with the CFATS program. In fiscal year 2019, the division had six primary goals and supporting objectives, including improving the effectiveness of the division's operations to reduce the risk to the nation from terrorist exploitation of chemicals at high-risk facilities and continuing to drive division process improvement and efficiencies.

[53]One of the CFATS program's supporting objectives deals with cybersecurity. Specifically, the program will seek to enhance connectivity and information sharing with the National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC's mission is to reduce the risk of systemic cybersecurity and communications challenges as the nation's flagship cyber defense, incident response, and operational integration center.

[54]The inspector-to-facility ratio ranges from 25-to-1 to 13-to-1 as of 2019, based on our analysis of the number of covered facilities and the program's inspector full-time equivalents. As previously mentioned, the CFATS program had 147 inspector full-time equivalents.

of the program's personnel documents. CFATS officials told us that the program's current staffing priority is to fill the vacant cyber analyst position, although they noted that this priority was based on broader program needs rather than those specifically related to its cybersecurity efforts.

However, several aspects of the CFATS program's staffing, inspection, and outreach efforts indicate the importance of addressing its cybersecurity workforce planning needs:

- **Cybersecurity tasks and knowledge, skills, and abilities for inspectors.** In 2018, the CFATS program identified two tasks and three knowledge, skills, and abilities related to cybersecurity for the inspector position as part of a DHS-wide effort to identify, categorize, and assign employment codes to its cybersecurity workforce, based on our review of Cybersecurity and Infrastructure Security Agency human capital documentation.[55] A Cybersecurity and Infrastructure Security Agency official told us that as of January 2020 the agency was in the process of updating position descriptions based on the assigned codes and was focused on updating vacant positions. By incorporating the identified cybersecurity knowledge, skills, and abilities that inspectors need to perform their duties into its workforce planning processes, the CFATS program can ensure that it has a workforce better capable of assessing the cybersecurity posture of covered facilities.
- **Linkage of facility cyber integration levels and workforce needs.** Although the CFATS program does not incorporate cybersecurity into its workforce planning, a facility's cyber integration level is used to determine the type of inspection staff assigned to inspect the facility, according to program guidance documents. Specifically, as mentioned earlier, facilities that are designated at the partial integration level require an inspector with additional training in cybersecurity or a headquarters-based cyber analyst to conduct the cybersecurity portion of the inspection. For facilities designated at the significant

[55]As previously mentioned, DHS components are required to identify, code, and track its cybersecurity workforce in accordance with the Homeland Security Cybersecurity Workforce Assessment Act and Cybersecurity Workforce Assessment Act of 2015, and guidance from the Office of Personnel Management. See Pub. L. No. 113-277, § 4, 128 Stat. 2995, 3008 (2014); Pub. L. No. 114-113, div. N, tit. III, § 303, 129 Stat. 2242, 2975. In 2018, the Cybersecurity and Infrastructure Security Agency reviewed and coded every position in the agency based on the National Institute of Standards and Technology's National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework).

integration level, a headquarters-based cyber analyst is required to conduct the cybersecurity portion of the inspection, according to program guidance documents. CFATS officials told us that cyber analysts are not required to physically attend inspections at facilities designated at the partial or significant integration levels but must either virtually or physically attend inspections at the significant integration level.

They also provided varying perspectives on the role a facility's cyber integration level played in determining the staffing of inspectors and cyber analysts. For example, a headquarters official and a supervisory inspector told us that integration levels do not play a role in determining the assignment of inspection staff. Additionally, one regional official told us that two inspectors are assigned to review facilities designated at the partial or significant cyber integration levels to assist with the cybersecurity portion of the review in their region. However, we observed a CFATS inspection in the official's region, and one inspector was assigned to review a facility designated at the partial integration level. Another regional official said that typically an inspector is able to manage the cyber portion of the inspection without the help of the cyber analyst, including for facilities designated at the partial or significant integration levels. By evaluating inspection staffing needs based on facility cyber integration levels and developing strategies to address these needs, the CFATS program can help ensure that it has the workforce capacity to conduct cybersecurity reviews of covered chemical facilities in each of its regional branches.

- **Role of cybersecurity experts.** As previously mentioned, the CFATS program has three expert cyber analyst FTEs to support its cybersecurity efforts. These analysts are to be responsible for reviewing inspection reports and providing cyber expertise as needed, based on our review of analyst position descriptions and interviews with CFATS officials. In addition to supporting inspections, cyber analysts can serve as a resource for inspectors and provide assistance if an inspector has technical questions or issues. They also may work directly with facilities on technical consultations. Cyber analysts also may work with chemical industry associations and member companies to share cybersecurity-related threat information and risk mitigation strategies, which are also passed down to facilities.

  Additionally, they are to help develop the program's policy, guidance, and training related to cybersecurity. However, CFATS officials provided varying perspectives on the support cyber analysts provide to inspectors. For example, a supervisory inspector told us that he

relays inspector questions or requests for support related to cybersecurity to CFATS officials at headquarters because of the limited number of cyber analysts. He stated that he has not made any requests for a cyber analyst to assist with an inspection, and, in general, if an inspector needs support with the cybersecurity portion of an inspection, another inspector with cybersecurity expertise will assist. Another inspector said that he does not coordinate or interact with cyber analysts on inspections, inspection reports, or other program-related work. By evaluating and addressing the cybersecurity efforts of cyber analysts into its workforce planning processes, the CFATS program can help ensure that it has capacity to provide the cybersecurity expertise needed to support the program's inspections and chemical industry outreach.

DHS workforce planning guidance outlines a process for its components to plan for its workforce needs. As part of this process, components should conduct a supply and demand analysis to identify gaps in capacity and capability and develop an action plan that includes strategies and efforts to address identified gaps. Previously, we and DHS's Office of the Inspector General found that DHS had not fully met statutory requirements to assess its cybersecurity workforce and develop a strategy to address workforce gaps.[56] In particular, DHS did not fully identify the readiness, capacity, and training needs of its workforce in its cybersecurity assessment and provided an incomplete cybersecurity workforce strategy to Congress.

Without addressing cybersecurity as part of its workforce planning, the CFATS program cannot ensure that it has the appropriate number of staff needed to carry out the program's cybersecurity-related efforts, including inspections, inspection report and approval reviews, and outreach to the chemical industry. In particular, the program cannot ensure that it has the appropriate number of inspectors positioned across its regional branches with the knowledge, skills, and abilities needed to assess the cybersecurity posture of covered chemical facilities. This raises the risk that the program does not have the workforce capacity and capability needed to ensure that covered chemical facilities have implemented adequate cybersecurity measures in the face of ever-expanding cybersecurity threats. By incorporating cybersecurity into its workforce planning processes, the CFATS program will be able to determine its

[56]GAO-18-466; Department of Homeland Security Office of Inspector General, *DHS Needs to Improve Cybersecurity Workforce Planning*, OIG-19-62 (Washington, D.C.: September 2019).

cybersecurity skills and staffing needs at the headquarters and regional levels and develop a plan to address them.

CFATS Does Not Track Information Key to Conducting Effective Workforce Planning for Cybersecurity

The CFATS program does not have a process to readily access or track data on the cyber integration levels of covered chemical facilities at the headquarters or regional level, which, as previously mentioned, are used to determine the type of inspection staff assigned to conduct or assist with an inspection.[57] CFATS officials told us that their inspection report database system does not have the capability to search for and extract this information because it is contained in the narrative section of these reports. Inspectors verify the cyber integration levels of facilities in authorization and compliance inspection reports, including any changes to the integration levels. To locate information about a facility's cyber integration level, a CFATS official explained that one would have to manually pull each inspection report and review the narrative. Officials said that they developed a draft request to contractors supporting their database system, requesting that they update their database system to allow staff to readily access and track cyber integration levels. However, they stated that this request was unofficial, and CFATS officials were unable to provide information on when it would be completed.

Additionally, CFATS officials may not have complete information on the capability of inspectors to conduct the cybersecurity portion of inspections. As a result, the program is unable to verify that inspectors in all of its regions have the capability to accurately assess the cybersecurity posture of covered chemical facilities and identify cyber vulnerabilities that could be addressed. For example, CFATS officials provided contrasting perspectives on the number and ability of inspectors to conduct these reviews, particularly for facilities designated at the partial or significant integration levels. CFATS officials at headquarters estimated that about 80 percent of the CFATS inspectors are capable of performing inspections at facilities designated at the partial integration level. They also said that there may not be a trained cybersecurity inspector in each of the program's 10 regions or in every state because the program's

[57]According to CFATS program's standard operating procedures for security plan reviews, facilities that are designated at the partial integration level require an inspector with additional training in cybersecurity or a headquarters-based cyber analyst to conduct the cybersecurity portion of the inspection. For facilities designated at the significant integration level, a headquarters-based cyber analyst is required to conduct the cybersecurity portion of the inspection or to support the review.

cybersecurity training was offered on a voluntary basis.[58] One inspector told us that many inspectors do not know how to determine a facility's cyber integration level because they lack cybersecurity expertise. He also said that inspectors have different criteria by which they determine a facility's cyber integration level and, in particular, there is inconsistency among inspectors about the characteristics of a facility designated at the significant versus partial cyber integration level. In contrast, a supervisory inspector told us that all of the inspectors in his region are at the full performance level and have the requisite training to review facilities at every integration level.

According to leading practices for human capital management, valid and reliable data are critical to assessing an agency's workforce requirements. This information heightens an agency's ability to manage risk by allowing managers to spotlight areas for attention before crises develop and identify opportunities for enhancing agency results.[59] The types of data that may inform workforce planning efforts may include a knowledge, skills, and competencies inventory for employees and the number of employees who received training, among others. With complete information about the level of cyber integration at covered chemical facilities, the CFATS program could better identify and track information critical to evaluating its workforce planning needs. Additionally, the program could better ensure that the appropriate inspectors are conducting these reviews and accurately assessing the cybersecurity posture of covered chemical facilities.

Conclusions

A successful cyberattack against chemical facilities' information and process control systems can disrupt or shut down operations and lead to serious consequences, such as health and safety risks, including substantial loss of life. The chemical sector's increasing reliance on these systems to more efficiently control and automate the production and use of hazardous chemicals combined with the rise in adversaries' efforts to manipulate and exploit vulnerabilities via evolving techniques, such as malware, and others, illustrates the importance of ensuring that high-risk

[58]Based on our review of the program's training and personnel documents, approximately 61 percent (83 of 136) of inspectors completed the "partial" training course—the only formal training course the program offered that specifically addressed cybersecurity.

[59]GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: March 2002).

chemical facilities are fully prepared to sustain and recover from these types of attacks.

While the CFATS program has taken steps to assist high-risk chemical facilities in their efforts to improve their cybersecurity posture, it does not have a process to ensure that it is sharing current, timely, and relevant guidance with industry so that covered chemical facilities can plan accordingly and protect their critical cyber assets with the most effective and efficient technological advances from attack. Moreover, CFATS inspectors may not be fully equipped with the skills needed to perform cybersecurity assessments at these facilities because the program has not fully incorporated several leading practices that GAO identified as key for effective training programs; incorporated cybersecurity needs into its workforce planning processes; or tracked cyber-related workforce data. As a result, CFATS inspectors that are evaluating a facility's cybersecurity posture may not have the knowledge, skills, and abilities to fully support the program's cybersecurity-related mission.

Recommendations

We are making the following six recommendations to the Cybersecurity and Infrastructure Security Agency:

The Assistant Director of the Infrastructure Security Division should implement a documented process for reviewing and, if deemed necessary, revising its guidance for implementing cybersecurity measures at regularly defined intervals. (Recommendation 1)

The Assistant Director of the Infrastructure Security Division should incorporate measures to assess the contribution that its cybersecurity training is making to program goals, such as inspector- or program-specific performance improvement goals. (Recommendation 2)

The Assistant Director of the Infrastructure Security Division should track delivery and performance data for its cybersecurity training, such as the completion of courses, webinars, and refresher trainings. (Recommendation 3)

The Assistant Director of the Infrastructure Security Division should develop a plan to evaluate the effectiveness of its cybersecurity training, such as collecting and analyzing course evaluation forms. (Recommendation 4)

The Assistant Director of the Infrastructure Security Division should develop a workforce plan that addresses the program's cybersecurity-related needs, which should include an analysis of any gaps in the program's capacity and capability to perform its cybersecurity-related functions, and human capital strategies to address them. (Recommendation 5)

The Assistant Director of the Infrastructure Security Division should maintain reliable, readily available information about the cyber integration levels of covered chemical facilities and inspector cybersecurity expertise. This could include updating the program's inspection database system to better track facilities' cyber integration levels. (Recommendation 6)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS officials, who provided written comments, which are reproduced in appendix I. In its comments, DHS concurred with our recommendations and described actions planned to address them. DHS also provided technical comments, which we incorporated as appropriate. We provided draft excerpts of this product to the American Chemistry Council, The Chlorine Institute, Institute of Makers of Explosives, National Association of Chemical Distributors, Society of Chemical Manufacturers and Affiliates, and the two chemical companies that we interviewed. For those who provided technical comments, we incorporated them as appropriate.

With regard to our first recommendation, that CISA should implement a documented process for reviewing and, if deemed necessary, revising its guidance for implementing cybersecurity measures at regularly defined intervals, DHS stated that CISA's Infrastructure Security Division (ISD) will work to develop a documented process for reviewing CFATS cybersecurity guidance at regularly defined intervals. DHS stated in its comments that once the process is documented and implemented, ISD will revise or supplement existing guidance, as appropriate. DHS also stated in its comments that CISA reviewed the cybersecurity guidance in May 2014 comparing the cybersecurity standard with the NIST Framework. DHS further stated in its comments that CISA considered updating the CFATS cybersecurity guidance based on the findings of a chemical security working group that was launched in February 2019. DHS stated in its comments that updating the guidance document can be a time-consuming process that would likely require public notice and comment. Therefore, according to DHS's comments, CISA instead is considering alternative ways to enhance the cybersecurity guidance provided to chemical facilities in a timelier manner. However, as we state in our report, despite the availability of recent guidance and other tools, the CFATS program does not have a process to routinely or periodically update its performance standards guidance that regulated chemical facilities and CFATS inspectors use to help implement the cybersecurity standard. Given the rapid changes in the current cybersecurity landscape, especially in relation to the increasing frequency and sophistication of cyberattacks against process control systems and evolving cyber threats overall, it is important that the CFATS program have a process to ensure at regularly defined intervals that it is sharing current, timely, and relevant guidance with industry so that covered chemical facilities can plan accordingly and protect their critical cyber assets from attack.

With regard to our second recommendation, that CISA incorporate measures to assess the contribution that its CFATS cybersecurity training

is making to program goals, DHS stated that CISA's ISD agrees that it is important to ensure training supports program goals, whether relating to inspector-specific or program-specific performance maintenance or improvement goals. Regarding inspector performance maintenance or improvement, DHS stated that, among other things, management will ensure that each inspector's individual performance plan fully captures their expected performance goals in the area of cybersecurity. DHS also stated that CISA's ISD will include mission goals specifically relating to cybersecurity in the section of the CISA Chemical Security 2021 annual operating plan section, which will be used to establish measures of performance levels and/or expected improvement for CFATS-related cybersecurity activities. These actions, if fully implemented, would be helpful, but taking additional steps, such as establishing a performance measure that relates directly to how cybersecurity training may be contributing to CFATS programmatic goals, would give CISA further assurance that its cybersecurity training is supporting the CFATS mission.

With regard to our third recommendation, that CISA track delivery and performance data for its cybersecurity training, DHS stated that CISA's ISD agrees that process improvements to better document and evaluate the effectiveness of the training provided to CFATS staff are worthwhile. DHS stated in its comments that CISA will establish policies and procedures intended to ensure that all cybersecurity training provided to chemical security personnel is accounted in a centralized mechanism. This accounting would include data on course attendance and completion and, where applicable, test scores received during the coursework and certifications gained, according to DHS's comments. These actions, if fully implemented, should address the intent of the recommendation.

With regard to our fourth recommendation, that CISA develop a plan to evaluate the effectiveness of its cybersecurity training, DHS stated that evaluating the effectiveness of training is beneficial and CISA's ISD will work to ensure that all cybersecurity courses provided to CISA chemical security staff are evaluated for effectiveness. DHS also stated that, among other things, CISA will require course evaluation forms from each attendee of any cybersecurity training provided by CISA to its chemical facility staff. Also, CISA will consider alternatives for obtaining required evaluation forms from chemical security staff, following their completion of non-DHS cybersecurity courses that are paid for by DHS. These actions, if fully implemented, should address the intent of the recommendation.

With regard to our fifth recommendation, that CISA develop a workforce plan that addresses the program's cybersecurity-related needs, DHS

stated that CISA's ISD will develop a concept of operations, which will include goals and requirements for a workforce review and planning effort to ensure the organization addresses the new program's capacity and capability to perform its regulatory, voluntary, and programmatic goals, to include its cybersecurity related functions. These actions, if fully implemented, should address the intent of the recommendation.

With regard to our sixth recommendation, that CISA maintain reliable, readily available information about the cyber integration levels of covered chemical facilities and inspector cybersecurity expertise, DHS stated that CISA's ISD retains information on cyber integration levels for regulated facilities but that it is not in a readily accessible format. DHS stated in its comments that ISD will execute a contract for new information technology development support for the CSAT system which, once executed, will work with the new support contractor to build a tool to automate the locating and reporting of a facility's cyber integration level data in a more accessible format. Additionally, DHS stated that with regard to making information on inspector cybersecurity expertise more readily available, ISD will require the Chief Learning Officer to maintain cybersecurity training information in a centralized repository of training and certification information for chemical security staff. These actions, if fully implemented, should address the intent of the recommendation.

We are sending copies of this report to the appropriate congressional committees, the Acting Secretary of the Department of Homeland Security, and other interested parties. 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 Nathan Anderson at (206) 287-4804 or AndersonN@gao.gov, and Nick Marinos at (202) 512-9342 or marinosn@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Nathan J. Anderson
Director, Homeland Security and Justice

Nick Marinos
Director, Information Technology and Cybersecurity

List of Requesters

The Honorable Gary Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

The Honorable Cedric L. Richmond
Chairman
The Honorable John Katko
Ranking Member
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
Committee on Homeland Security
House of Representatives

The Honorable James Langevin
Committee on Homeland Security
House of Representatives

Appendix I: Comments from the Department of Homeland Security

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

Homeland Security

May 1, 2020

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

Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO 20-453, "CRITICAL INFRASTRUCTURE PROTECTION: Actions Needed to Enhance DHS Oversight of Cybersecurity at High-Risk Chemical Facilities"

Dear Messrs. Anderson and Marinos:

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

DHS's Cybersecurity and Infrastructure Security Agency (CISA) manages the Chemical Facility Anti-Terrorism Standards (CFATS) Program, the principal mechanism by which the Department works with the chemical industry and other stakeholders to prevent the misuse of chemicals and attacks on the nation's chemical infrastructure. CFATS accomplishes this by requiring high-risk chemical facilities to implement appropriate physical and cyber security measures, which CISA Chemical Security Inspectors subsequently verify during onsite inspections. Throughout the history of the CFATS program, CISA has taken several actions to ensure CFATS-related cybersecurity guidance is practical and useful, and that CFATS staff responsible for reviewing compliance with cybersecurity standards are properly trained.

Cybersecurity is an integral part of the DHS's national approach to chemical security. The Department remains committed to ensuring that high-risk chemical facilities are implementing appropriate physical and cyber security measures.

The draft report contained six recommendations with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments 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: 2020.05.01 08:04:55 -04'00'

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

Attachment

2

Attachment: DHS Management Response to Recommendations Contained in GAO 20-453

GAO recommended that the Assistant Director of the Infrastructure Security Division (ISD):

Recommendation 1: Implement a documented process for reviewing and, if deemed necessary, revising its guidance for implementing cybersecurity measures at regularly defined intervals.

Response: Concur. CISA's ISD acknowledges the benefits of reviewing CFATS cybersecurity guidance on a recurring basis and has done so multiple times, resulting in the provision of updated, supplemental guidance to CFATS-regulated facilities and staff on several occasions. ISD will work to develop a documented process for reviewing CFATS cybersecurity guidance at regularly defined intervals. Once the process is documented and implemented, ISD will revise or supplement existing guidance, as appropriate. It is important to note, however, that previous reviews found the CFATS cybersecurity guidance generally sufficient.

In May 2014, for example, following the release of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, CISA's ISD completed an analysis between the CFATS Risk-Based Performance Standard (RBPS) on cybersecurity (RBPS-8) and the NIST Framework. The analysis did not find significant cybersecurity gaps between the two programs. A summary of the results of the CFATS RBPS-8/NIST cybersecurity framework is available on CISA's public website at https://www.cisa.gov/publication/eo-13636-improving-ci-cybersecurity.

Additionally, CISA's ISD Assistant Director established a Chemical Security Modernization Working Group (CSMWG) during February 2019 to assess CISA's chemical security activities. CSMWG activities included a review of the CFATS cybersecurity guidance, as well to identify potential ways of improvement. Based on the findings of the working group, CISA considered updating the CFATS RBPS guidance on cybersecurity. However, as updating the guidance document can be a time-consuming process that would likely require public notice and comment, CISA instead is considering alternative ways to enhance the cybersecurity guidance provided to chemical facilities in a timelier manner. This could include the issuance of updated supplemental cybersecurity materials separate from the CFATS RBPS guidance document, such as the 2017 "CFATS RBPS-8 Cyber Fact Sheet," available at https://www.cisa.gov/publication/cfats-rbps-8-cyber, and the 2015 "Chemical Sector Cybersecurity Framework Implementation Guide," available at https://www.cisa.gov/publication/chemical-cybersecurity-framework-implementation-guidance." Estimated Completion Date (ECD): December 31, 2020.

3

Recommendation 2: Incorporate measures to assess the contribution that its cybersecurity training is making to program goals, such as inspector- or program-specific performance improvement goals.

Response: Concur. CISA's ISD agrees that it is important to ensure training supports program goals, whether relating to inspector-specific or program-specific performance maintenance or improvement goals. Regarding inspector performance maintenance or improvement, management will ensure that each inspector's individual performance plan fully captures their expected performance goals in the area of cybersecurity. Also, performance will be assessed through classroom testing during the classroom training phase, and subsequently through the CFATS auditing program during actual inspections in the field. Each inspectors' performance results will then be reviewed by management to assess their current performance level and determine whether additional training is recommended and/or if the training requires correction.

Finally, CISA's ISD will also include mission goals specifically relating to cybersecurity in the section of the CISA Chemical Security 2021 annual operating plan section. This will be used to establish aggressive but realistic measures of performance levels and/or expected improvement for CFATS-related cybersecurity activities. ECD: December 31, 2020.

Recommendation 3: Track delivery and performance data for its cybersecurity training, such as completion of courses, webinars, and refresher trainings.

Response: Concur. CISA's ISD agrees that process improvements to better document and evaluate the effectiveness of the training provided to CFATS staff are worthwhile. It is important to note, however, that CFATS inspectors and compliance staff receive significant—and evolving—cybersecurity training throughout the lifetime of the CFATS program. For example, GAO's draft report notes that nearly a dozen different cybersecurity training activities provided to CFATS inspectors in the course of the program either partially or generally meets all four of GAO's categories of best practices for training.

Currently, CISA's ISD is updating beginner and intermediate cybersecurity training for CFATS inspectors. During the training's design and piloting, CISA took steps which address the intent of this recommendation. For example, CISA is incorporating mechanisms to track and document who receives the training, as well as ensuring that specific learning objectives were met. At the conclusion of the training, recipients will have the opportunity to evaluate the training, which is then incorporated into future training initiatives.

CISA currently uses the DHS Performance and Learning Management System (PALMS) to track the majority of training completed by its personnel. Moving forward, CISA will

establish policies and procedures intended to ensure that all cybersecurity training provided to chemical security personnel is accounted in the DHS PALMS system, or another centralized mechanism. This will include data on course attendance and completion and, where applicable, test scores received during the coursework and certifications gained. CISA ISD will also work to ensure centralized tracking, either in DHS PALMS or elsewhere, of cybersecurity webinars and refresher trainings provided to chemical security staff. ECD: December 31, 2020.

Recommendation 4: Develop a plan to evaluate the effectiveness of its cybersecurity training, such as collecting and analyzing course evaluation forms.

Response: Concur. Evaluating the effectiveness of training is beneficial and CISA's ISD will work to ensure that all cybersecurity courses provided to CISA chemical security staff are evaluated for effectiveness. ISD will require course evaluation forms from each attendee of any cybersecurity training provided by CISA to its chemical facility staff. Also, CISA will consider alternatives for obtaining required evaluation forms from chemical security staff, following their completion of non-DHS cybersecurity courses that are paid for by DHS. Evaluation forms for both DHS and non-DHS cybersecurity classes provided to chemical security staff will be analyzed by CISA to determine: (1) the efficacy of each course; (2) what changes may be needed for DHS-provided courses; or (3) whether DHS should continue to pay for external courses. In addition to course evaluations, ISD will leverage the existing CISA chemical security audit program to evaluate the effectiveness of any provided cybersecurity course in improving the performance of chemical security inspectors and cyber analysts. ECD: December 31, 2020.

Recommendation 5: Develop a workforce plan that addresses the program's cybersecurity-related needs, which should include an analysis of any gaps in the program's capacity and capability to perform its cybersecurity-related functions, and human capital strategies to address them.

Response: Concur. CISA's ISD will develop a concept of operations, which will include goals and requirements for a workforce review and planning effort to ensure the organization addresses the new program's capacity and capability to perform its regulatory, voluntary, and programmatic goals, to include its cybersecurity related functions.

CISA is also updating position descriptions (PDs) for existing vacancies. As part of this, CISA will conduct a review of the applicable PDs to ensure the positions that require cybersecurity expertise include those requirements in the requisite PDs. ECD: December 31, 2020.

5

Recommendation 6: Maintain reliable, readily available information about the cyber integration levels of covered chemical facilities and inspector cybersecurity expertise. This could include updating the program's inspection database system to better track facilities' cyber integration levels.

Response: Concur. While CISA's ISD currently retains information on the cyber integration level for all regulated facilities; at present, that information is not in a readily accessible format. Specifically, this information is in text fields of facility reports stored within CISA's Chemical Security Assessment Tool (CSAT), which is not easily searchable. ISD will execute a contract for new information technology development support for the CSAT system which, once executed, will work with the new support contractor to build a tool to automate the locating and reporting of a facility's cyber integration level data in a more accessible format. Also, CISA is exploring the possibility of updating its Top-Screen to include a question concerning a facility's cyber integration level data, which would also make the data on cyber integration levels more readily available.

With regard to making information on inspector cybersecurity expertise more readily available, ISD will require the Chief Learning Officer to maintain cybersecurity training information in a centralized repository of training and certification information for chemical security staff.

ECD: October 31, 2021.

6

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Nathan J. Anderson at (206) 287-4804 or andersonN@gao.gov
Nick Marinos at (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the contact above, Ben Atwater (Assistant Director), Michael W. Gilmore (Assistant Director), Nanette Barton (Analyst-in-Charge), Chuck Bausell, Benjamin Crossley, Clifton Douglas, Jr., Michele Fejfar, Tracey King, Ryan Lester, Thomas Lombardi, Dennis Mayo, Cassaundra Pham, Corinne Quinones, and Kevin Reeves made key contributions to this report.