

Chemical Security: DHS Should Provide Options for Voluntary Vetting of Facility Personnel for Terrorist Ties

GAO-26-108127

Q&A Report to the Chair, Committee on Homeland Security, House of Representatives

September 8, 2026

Accessible Version

Why This Matters

Chemicals play a vital role in U.S. manufacturing and impact the lives of Americans every day. According to the Department of Homeland Security (DHS), chemicals are used to produce 96 percent of all U.S. manufactured goods. To support this role, DHS estimated that in 2023 the U.S. had approximately 45,000 facilities that produced, used, or stored hazardous chemicals, some of which terrorists could use to inflict mass casualties and damage. DHS estimates that, as of 2025, more than 89 million people live or work within 2 miles of facilities using high-risk chemicals. If released, stolen, or diverted and used to create explosive devices or otherwise weaponized, DHS officials estimate that these chemicals could cause significant harm to the surrounding populations, ranging from fatalities at the facility to the equivalent impact of a nuclear explosion. Securing the chemical sector is therefore a key component of the nation's critical infrastructure protection efforts.

DHS's Cybersecurity and Infrastructure Security Agency (CISA) leads the nation's efforts to secure and protect the nation's 16 critical infrastructure sectors—including the chemical sector—against risks. These sectors cover infrastructure areas vital to U.S. security and economic and public health.

You asked us to examine DHS's efforts to mitigate security risks to the U.S. chemical sector. We are providing information on CISA's past regulatory program for chemical facility security and our examination of CISA's present efforts to address its responsibilities to mitigate security risks to the chemical sector.

Key Takeaways

- CISA officials and selected chemical sector representatives from the private sector cited the lack of a federal terrorist vetting program for chemical facility personnel, following the lapse of the past chemical facilities regulatory program, as a key security challenge.
- CISA officials reported that reductions in personnel taken in 2025 have necessitated that the agency reduce or eliminate services it originally established as part of the past regulatory program. It has also reduced other activities and services, such as on-site facility assessments and cybersecurity incident support.
- Selected private sector chemical sector representatives stated that their contact with CISA regarding security vulnerabilities has declined following CISA's reductions in personnel and the resulting loss of long-standing points-of-contact and experienced staff with expertise in chemical security.
- We recommend that CISA should identify, evaluate, and implement options for chemical facility owners and operators to voluntarily vet facility personnel

and certain others for terrorist ties, and, if necessary, seek legislative authority to do so. CISA did not concur with our recommendation.

What is CISA's role in securing chemical facilities?

The Cybersecurity and Infrastructure Security Agency Act of 2018 provides that CISA is responsible for coordinating a national effort to secure and protect the nation's critical infrastructure against risks.¹ The nation's critical infrastructure is defined as systems and assets—physical or virtual—considered so vital that their incapacitation or destruction would debilitate national security, economic security, or public health or safety.²

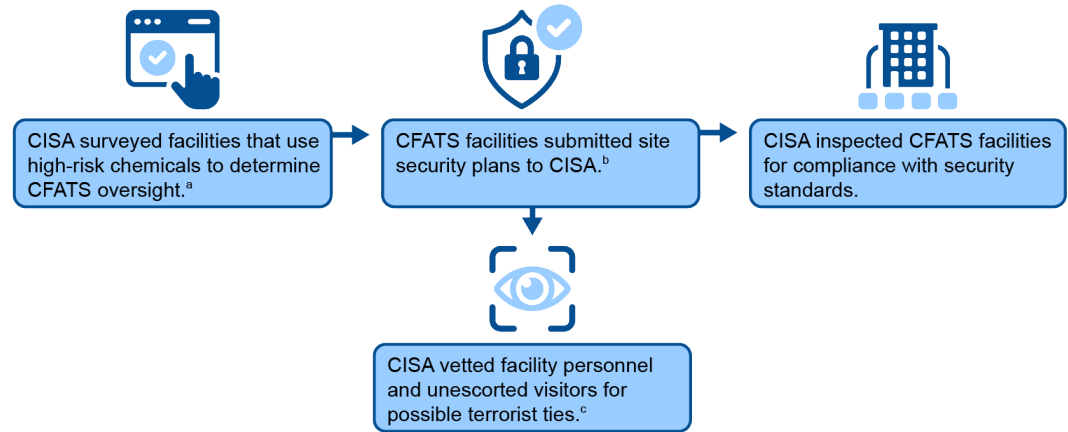
CISA is also the sector risk management agency (SRMA) for multiple critical infrastructure sectors, including the chemical sector. SRMAs, in general, are responsible for providing specialized sector-specific expertise to critical infrastructure owners and operators and supporting programs and associated activities within their sectors.³ (For a list of critical infrastructure SRMA roles and responsibilities, see appendix I.) As SRMA for the chemical sector, CISA is responsible for supporting sector risk management, including establishing and implementing programs to assist chemical facilities to identify, understand, and mitigate threats, vulnerabilities, and risks. The agency is also responsible for leading the day-to-day coordination of sector-specific activities, including chairing the chemical sector government coordinating council and working with the private sector coordinating council on sector issues.⁴ To carry out its responsibilities, CISA works in partnership with chemical facility owners and operators—which we also refer to as “chemical companies” in this report—to secure the sector.

What actions did CISA take to mitigate security risks to the chemical sector through CISA's past regulatory program for high-risk facilities?

In 2007, DHS established the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program; through CFATS, CISA took multiple actions to mitigate security risks to high-risk facilities.⁵ The CFATS program was intended to safeguard the security of the nation's chemical infrastructure by assessing the security risks U.S. high-risk chemical facilities pose. It also required high-risk facilities to meet 18 risk-based performance standards across various areas of security. As of 2023, CISA had designated about 3,200—7 percent—of the approximately 45,000 chemical facilities in the U.S. at that time as high-risk under the CFATS program. The CFATS program identified facilities at high-risk of experiencing significant consequences from a terrorist attack based primarily on the quantities and concentrations of dangerous chemicals the facilities possessed or planned to possess.⁶ In July 2023, the statutory authority for CFATS expired and the program was discontinued.

The CFATS program enabled CISA officials to take actions to mitigate security risks to the chemical sector. In addition to identifying high-risk facilities, CFATS established security performance standards and required facility inspections to assess whether those standards were in place. Figure 1 below shows selected key actions in the CFATS program.⁷

Figure 1: Selected Key Actions in the Cybersecurity and Infrastructure Security Agency's (CISA) Discontinued Chemical Facilities Anti-Terrorist Standards (CFATS) Program



Source: Analysis of CFATS documents. | GAO-26-108127

^aIn its regulations for the CFATS program, CISA listed certain dangerous chemicals as “chemicals of interest”—chemicals that could have significant consequences when used in a terrorist attack or other security incident at or above specific quantities or concentration thresholds. See 6 C.F.R. pt. 27, app. A.

^bThe owners and operators of high-risk chemical facilities covered by CFATS were required to create site security plans identifying the security measures their facilities would take to address CFATS’ 18 performance standards. CISA inspectors were to periodically inspect facilities to assess the extent to which they were complying with their security plans.

^cCFATS performance standards required high-risk chemical facilities to perform background checks on personnel and unescorted visitors with access to restricted areas or critical assets to identify people with terrorist ties. Facilities were to include how they planned to meet the requirement in their site security plans. Terrorist vetting was conducted under the CFATS Personnel Surety Program.

CFATS required owners and operators of high-risk facilities to develop a facility site security plan that identified security measures needed to comply with the program’s 18 performance standards, in areas such as perimeter security (as shown in fig. 2), access control, personnel surety, and cyber security. According to CISA officials, under the CFATS program, CISA officials were to inspect high-risk facilities every 2 years, to determine the extent to which the facilities were implementing their security plans. CISA was authorized to take enforcement actions, such as issuing an order for corrective action to a facility, if the facility was not in compliance with its approved site security plan.

Figure 2: Chemical Facility Perimeter Secured by Chain-Link Fencing and Razor Wire



Source: GAO. | GAO-26-108127

Note: This photograph shows how one chemical facility secures its perimeter and the chemicals within.

What did CISA determine to be the effects of discontinuing the CFATS program on chemical sector security?

As of June 2026, CISA officials told us that while the agency had not performed an assessment of the effects of discontinuing the CFATS program on sector security, they consider the effects to be the loss of security measures intended to mitigate the risk of dangerous chemicals being weaponized by terrorists. In the absence of CFATS, high-risk facility owners and operators are now responsible for determining the security needs of their own facilities, which may vary by facility, and implementing the security measures they put in place to meet those needs. According to CISA officials, private sector stakeholders communicated to them that discontinuing the CFATS program posed a significant risk for the chemical sector.

CISA officials identified the results of CFATS measures that ended when the CFATS program was discontinued. For example, the facility inspections that CFATS required identified security vulnerabilities that required immediate, on-site resolution or further technical consultation to address. According to CISA officials, these vulnerabilities included, for example, incomplete or unmonitored intrusion detection systems that could allow undetected trespassing, incomplete controls over improperly labeled hazardous chemicals, and missing or incomplete personnel background checks. CISA officials stated that without the CFATS regulatory program, the agency does not have the means to collect information to identify high-risk facilities, the authority to require facility owners and operators to perform their own security assessments, or the authority to undertake enforcement actions to address identified vulnerabilities.

In 2025, CISA officials stated that discontinuing CFATS also ended a key aspect of chemical facility security—the vetting of facility personnel and visitors seeking unescorted access to restricted areas or critical assets within a facility for possible terrorist ties through the CFATS’ Personnel Surety Program.⁸ (For the purposes of this report, when we refer to the vetting of chemical facility personnel for terrorist ties, we are including the vetting of any visitors seeking unescorted access to restricted facility areas or critical assets.) According to CISA officials, when authorization for the CFATS program expired in July 2023, the Personnel Surety Program was vetting, on a continuous basis, approximately 500,000 individuals.⁹ According to CISA officials, over the duration of CFATS, the program identified individuals who were on the U.S. government’s Terrorist Screening Dataset, commonly known as the “terrorist watchlist.”¹⁰ This watchlist is the government’s primary method to consolidate and share information on individuals who may pose terrorist threats to the U.S.

CISA officials also noted that when authorization for the CFATS program expired, CISA was no longer able to collect CFATS inspection-related data, which officials had used, along with other data, to identify and assess risks to the chemical sector. According to officials, the loss of these data left a gap in their collection of sector facility data. Officials said the agency used CFATS data to identify potential risk trends and areas in which additional CISA enforcement actions might be needed. The CFATS data included, for example, the number of facility enforcement actions (by enforcement category, such as “warnings”), number of personnel vetted for terrorist connections, types of facilities enrolled, and facilities’ geographic areas.

CISA officials told us they now use other data to analyze sector security, such as input from subject matter experts and source material on potential threats from other government agencies. We sought to review CFATS data collected prior to the discontinuation of the program; however, CISA no longer maintains these data in a readily accessible format that we could review.

What have CISA and sector stakeholders identified as the most significant security challenge for high-risk chemical facilities following the discontinuation of the CFATS program?

According to CISA officials and representatives from the private sector coordinating council, the three selected chemical associations, and the six selected chemical companies we interviewed, losing the Personnel Surety Program is the most significant challenge high-risk chemical facility owners and operators have faced following the discontinuation of the CFATS program.¹¹ CISA officials also stated that discontinuing the Personnel Surety Program left a gap in chemical facility security that poses significant risks.

The CFATS program required high-risk facilities covered by the program to perform background checks on personnel, including taking measures to identify individuals with terrorist ties. This requirement was designed to reduce the likelihood of an “insider threat”—defined as a security risk originating from within an organization—from facility personnel with the potential to cause significant harm through access to dangerous chemicals and critical cyber systems. According to DHS, identifying individuals with terrorist ties is an inherently governmental function and requires the use of information held in government-maintained databases that is unavailable to facility owners and operators; therefore, CISA implemented the Personnel Surety Program in 2015.¹²

Under the Personnel Surety Program, owners and operators had four options for ensuring their facility personnel were vetted against the terrorist watchlist.¹³

- **Option 1—direct vetting.** Permitted facility owners and operators to submit certain identifying information about their personnel—such as name and date of birth—directly to CISA.
- **Option 2—vetting conducted under other DHS programs.** Permitted facility owners and operators to use the vetting programs operated by other DHS agencies to vet their personnel for terrorist ties.¹⁴
- **Option 3—electronic verification through the Transportation Worker Identification Credential (TWIC).** Permitted facility owners and operators to use DHS’s TWIC program. TWIC, operated by the Transportation Security Administration (TSA), uses biometric technology to determine and verify an individual’s identity, such as through fingerprinting.
- **Option 4—visual verification of credentials.** Permitted facility owners and operators to visually verify on site the badge credentials issued to an individual as part of any federal program that periodically vets individuals for terrorist ties.¹⁵

Under the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021—the statutory authority that establishes critical infrastructure SRMAs’ responsibilities—SRMAs are to establish and carry out security programs to assist facility owners and operators in identifying and mitigating threats and vulnerabilities to their systems or assets (see app. I for a list of critical infrastructure SRMA responsibilities.)¹⁶

CISA officials told us that they do not have explicit authority to reinstate the Personnel Surety Program as it was formerly operated, and have not formally assessed whether CISA has the authority to establish other options for personnel vetting, such as a voluntary program, under its statutory authority as the chemical sector SRMA. However, as of May 2026, officials said they were exploring how CISA’s SRMA authority may be used to address security risks to the chemical sector, such as through personnel vetting, depending on the needs of stakeholders.

CISA officials said they recognize the importance of vetting facility personnel for terrorist ties but noted that there are a number of implementation challenges that the agency would need to address. For example, under CFATS, the number of facilities that participated in the mandatory Personnel Surety Program was limited to about 3,200 designated high-risk facilities, whereas the number of facilities participating in a voluntary program could be far greater, and that number could fluctuate. According to CISA officials, the unknown scope of a voluntary program could also make identifying and securing the resources CISA would need to operate the program challenging. Moreover, implementing such a program would also involve addressing privacy issues associated with the collection and use of personal identifiable information, such as Social Security numbers and dates of birth.

Identifying, evaluating, and implementing a process for the voluntary vetting of facility personnel for terrorist ties could present challenges. However, as the designer of this effort, CISA could determine the necessary scope and other parameters that would work best for the agency as well as the private sector, including size limitations and participation requirements. Identifying the scope would also help CISA identify the resources needed to operate the program. In terms of cost, for example, CISA obligated about \$500,000 per fiscal year to operate the Personnel Surety Program, for about 8 years starting from its launch to the discontinuation.

However, CISA officials also stated that the potential for an insider terrorist attack on a chemical facility is a significant risk because facility owners and operators cannot vet facility personnel for terrorist ties through a CISA program. To help mitigate the insider threat, CISA provides guidance and resources to chemical facility owners and operators on security best practices, such as tools designed to help owners and operators recognize and respond to insider threats. CISA officials also noted that despite these efforts, the gap in personnel vetting—that is, the lack of specific vetting for terrorist ties—poses significant risks to the sector for an insider terrorist attack.

Under CFATS, in addition to the direct vetting of personnel through CISA, the Personnel Surety Program offered chemical facility owners and operators options for using other existing federal vetting programs to meet the terrorist vetting requirement, such as DHS’s TWIC program. In the absence of the CFATS Personnel Surety Program, these existing federal vetting programs could again offer facility owners and operators options for vetting their facility personnel for potential terrorist ties.

Without federal options for vetting facility personnel and unescorted visitors for possible links to terrorism, CISA and chemical facility owners and operators lack a critical tool to help assure that their facilities are not at significant risk of an insider terrorist attack and from potential disruptions to critical national supply chains.

What actions did CISA take to address its SRMA responsibilities to mitigate security risks for the chemical sector following the CFATS program discontinuation?

In the absence of the CFATS program, CISA has taken various physical and cybersecurity actions to address its SRMA responsibilities to mitigate security risks to the chemical sector. (See app. I for a list of critical infrastructure SRMA responsibilities.) For example, CISA’s ChemLock is a voluntary program that offers owners and operators of facilities possessing potentially dangerous chemicals no-cost services and tools that address physical and cyber-related threats to help mitigate security risks. According to CISA officials, the agency began this program in 2021 as a pilot and expanded the range of services and tools available following the discontinuation of CFATS. ChemLock tools include on-site security assessments, security guidance, fact sheets, tailored tabletop exercises to assess facility security, personnel security training, and special access to related CISA services.

CISA also provided various other services to chemical facility owners and operators, such as classified and unclassified quarterly briefings, intelligence bulletins, sector briefings, scenario-based planning, and on-site facility simulation exercises. However, according to CISA officials, many of the services that required direct support, such as an assessment by a security advisor and certain ChemLock functions, were limited in 2025 due to resource constraints.

CISA officials said they continued to provide specialized expertise in identifying and mitigating cybersecurity risks for the chemical sector, as well as the other critical infrastructure sectors. CISA offered multiple no-cost cybersecurity services, guidance, and strategies for chemical sector owners and operators through various mechanisms. For example, as shown in Figure 3 below, through its website CISA provided ransomware and cyber hygiene guidance and services (vulnerability and web application scanning services); guidance on known cyber vulnerabilities, responses, and best practices; and guidance and strategies to protect network devices (routers, firewalls, and internet-facing servers). CISA officials told us they also provide on-site penetration testing and incident response support; however, they noted that as of May 2026, CISA has limited the latter services due to resource constraints.¹⁷



Source: Cybersecurity and Infrastructure Security Agency. | GAO-26-108127

How did CISA’s personnel resources for chemical sector security change from fiscal years 2024 to 2025?

As shown in table 1, CISA personnel available to directly support CISA chemical sector activities declined from 214 in fiscal year 2024 (96 percent of authorized positions) to 52 in fiscal year 2025 (25 percent of authorized positions).¹⁸ These active personnel did not include full-time personnel who were on administrative leave in fiscal year 2025 and scheduled to separate from the agency by the end of calendar year 2025 through deferred resignation programs.¹⁹ Authorized sector support positions from fiscal years 2024 to 2025 largely remained constant for the Infrastructure Security Division. However, authorized positions for the Integrated Operations Division—which conducts intelligence analyses and coordination—declined 11 percent from 143 positions to 127.

Table 1: Authorized CISA Full-Time Positions and Active Personnel Dedicated to Chemical Sector Security Activities and Programs, Fiscal Years 2024 and 2025

CISA division	Fiscal year	Number of full-time authorized positions	Number of active personnel	Percentage of authorized positions filled by active personnel
Infrastructure Security ^a	2024	81	71	88%
	2025	80	28	35%
Integrated Operations ^b	2024	143	143	100%
	2025	127	24	19%
Totals	2024	224	214	96%
	2025	207	52	25%

Source: GAO analysis of Cybersecurity and Infrastructure Security Agency (CISA) personnel data. | GAO-26-108127

Notes: These data represent authorized full-time positions and active full-time personnel—personnel not on administrative or other leave—dedicated to chemical sector security activities, as of the end of the fiscal years, September 30, 2024, and 2025. These authorized positions and personnel were assigned across two of CISA’s divisions. According to CISA officials, a third division—the Stakeholder Engagement Division—had three active personnel filling three positions dedicated to chemical sector security activities and programs at the end of fiscal years 2024 and 2025. This CISA division leads CISA’s national and international voluntary partnerships and engagements and serves as a hub for shared stakeholder—government and private-sector—information. Other CISA divisions may provide additional support, either directly or indirectly, for chemical sector activities, on an as-needed basis.

^aThis CISA division conducts and facilitates chemical facility vulnerability and consequence assessments and provides information on emerging threats and hazards to the chemical sector.

^bThis CISA division conducts, among other services, intelligence analyses and operates CISA Central. (CISA Central is a hub for critical infrastructure stakeholders to communicate with CISA regarding threats and emerging risks and to request information and assistance.) The division also partners with the U.S. intelligence community; and develops operational plans and readiness programs for CISA operational priorities, such as elections security.

What reported effects has a reduction in CISA personnel resources had on the agency's ability to address its SRMA responsibilities for the chemical sector?

CISA officials told us that the 2025 reductions in agency personnel necessitated that the agency re-evaluate its sector SRMA responsibilities and that the reductions affected its efforts to meet those responsibilities. According to officials, under the revised staffing levels, the agency cannot maintain the same level of sector support that it had been providing. In response to personnel reductions, the agency has reduced or eliminated services it originally established as part of the CFATS program, such as the support services of former program inspectors.

In 2025 and 2026, the number of other sector activities and services CISA initiated or attended substantially declined from prior calendar years. For example, while CISA has conducted a limited number of industry security conferences, tabletop exercises, and advanced security awareness training, it no longer provides inspector outreach and support for individual facilities. Officials also stated that the agency has paused coordination with local and international partners and has reduced its support of cybersecurity incidents. Additionally, CISA has greatly reduced the bulk of ChemLock services, such as most on-site assessments. However, the agency continues to offer advanced security training, cybersecurity guidance, and other services. CISA officials also told us that reductions in personnel included agency veterans with subject-matter expertise in chemical sector security risks and operations .

What are selected chemical sector owners and operators' views on CISA's level of support as a SRMA?

Representatives from the private sector coordinating council, the three chemical associations, and the six individual companies we interviewed stated that facility owners' and operators' trust in CISA has eroded due to the loss of long-standing relationships with agency points-of-contact and subject matter experts as a consequence of personnel reductions. They noted that their long-term agency points-of-contact were very knowledgeable about their individual facilities and about chemical security in general. They also said that those close relationships with the agency's points-of-contact had allowed them to candidly discuss potential security vulnerabilities without fear of being sanctioned by CISA officials.

Representatives from the three chemical associations and the six companies also stated that facility owners and operators no longer knew who to contact at CISA to answer their security questions, get state or local first responder agency referrals, or obtain help with other security needs, because they no longer had agency points-of-contact. For example, representatives from one company stated that prior to the agency's personnel reductions, their CISA point-of-contact had been invaluable in rapidly coordinating response efforts to a fire started by an illegal campfire outside one of their facilities, which spread to the perimeter fence. Their CISA contact coordinated a multi-pronged response effort that included local and state first responders (police, fire department, hazmat containment, and social services) as well as representatives from the railroad company that owned the adjacent property. Company representatives noted that without CISA's support and expertise, they would not have known who to contact to arrange the needed coordinated response.

What efforts has CISA undertaken to assess chemical sector risks and develop a plan to address those risks?

In February 2025, according to CISA officials, CISA completed the draft of an assessment of risks to the chemical sector and a risk management plan to address identified risks.²⁰ As of May 2026, CISA officials told us that they did not have timeframes for issuing the reports.²¹ CISA's last documented assessment of chemical sector risk and mitigation planning was completed in 2015, although officials stated that they generally update DHS with information on priority critical infrastructure, including chemical facilities.

In June 2024, CISA provided a risk assessment template and guidance to all critical infrastructure SRMAs to use in drafting a sector-specific risk assessment for their sectors, including the chemical sector.²² According to CISA officials, to develop the assessment, they coordinated with sector partners, such as the private sector coordinating council, and identified and assessed seven risk scenarios.²³ They also said that CISA initiated the chemical sector risk assessment and risk management plan in response to directives in the *National Security Memorandum on Critical Infrastructure Security and Resilience/NSM-22*. This memorandum, issued by the prior administration in April 2024, required all critical infrastructure SRMAs to assess sector risks and recommend specific risk mitigation measures.²⁴ According to CISA officials, the current administration is in the process of reviewing this memorandum, and both the chemical sector draft assessment and management plan are on hold until the review is completed.²⁵

CISA officials said CFATS program data, as well as information from subject matter experts, informed their understanding of risks and consequences of chemical facility security incidents, as addressed in the draft sector risk assessment. Additionally, officials explained that they used data and other inputs from subject matter experts within other federal agencies, such as the Environmental Protection Agency and the Federal Bureau of Investigation. These officials said they researched and analyzed source materials from across the federal government to assess the likelihood and consequences of identified risks to the chemical sector.

Conclusions

Given the potential for high-risk chemicals to inflict mass casualties and damage when weaponized, ensuring the security of the facilities that use these chemicals is critical. Following the discontinuation of the CFATS program, high-risk chemical facility owners and operators have assumed responsibility for determining their facility security needs and implementing security measures. However, one security measure they cannot implement on their own is vetting their personnel—and other individuals seeking unescorted access to restricted areas or critical assets—for terrorist ties. As SRMA for the chemical sector, CISA—as well as private sector stakeholders—have identified the terrorist insider threat as a significant security gap for the sector, but the agency has yet to determine how to address this gap, such as through providing options for voluntary terrorist watchlist vetting. While identifying, evaluating, and implementing voluntary options to vet facility personnel could present challenges, without government support to enable the vetting of facility personnel, facility owners and operators lack a key tool to protect their facilities from an insider terrorist attack, which could have potential disruptions to critical national supply chains.

Recommendation for Executive Action

The Director of CISA should identify, evaluate, and implement voluntary options for chemical facility owners and operators to address insider terrorist security risks by vetting their personnel and unescorted visitors with access to restricted areas or critical assets, and, if necessary, seek the legislative authority to do so. (Recommendation 1)

Agency Comments

We provided a draft of this product to DHS for review and comment. DHS provided written comments, which are summarized below and reproduced in appendix II. DHS also provided technical comments, which we incorporated as appropriate. In its written comments, DHS did not concur with our recommendation.

After we sent our report for comment, in response to feedback from CISA, we adjusted the wording of the recommendation to clarify that CISA should take the intermediary steps of identifying and evaluating options for chemical facilities to vet their personnel for possible terrorist ties, and made adjustments to the report language as appropriate.

Regarding DHS's written comments, we acknowledge that instituting options for voluntary personnel vetting without the support of a regulatory framework could raise complex legal and practical implementation issues. However, the information we collected and the sector stakeholders we interviewed for this review—including CISA officials—demonstrated that facilities' inability to vet their personnel for terrorist ties is a security gap that presents substantial risks. These risks were evidenced by the individuals CISA's prior regulatory program identified as having terrorist ties. The private sector cannot address this security gap on its own because it cannot independently access the terrorist watchlist, the critical component in terrorist vetting. Given that chemical facility owners and operators lack a key tool to protect their facilities from an insider terrorist attack and that, without vetting, CISA's current security activities cannot fully mitigate this threat, we continue to believe that CISA should identify, evaluate, and implement voluntary options for facilities to vet their personnel for terrorist ties—as it has in the past—and, if necessary, seek legislative authority to do so.

How GAO Did This Study

To conduct this work, we reviewed relevant statutes and CISA guidelines, and also analyzed the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22). However, we did not include it in our study because CISA officials told us it was on hold at the time of our work, pending review by the administration; we therefore focused on relevant statutory requirements.²⁶

We explored analyzing the CFATS program data that CISA officials told us they had used to assess the effects of discontinuing the CFATS program, such as number of facility inspections and enforcement violations. We assessed the reliability of these data by analyzing CISA's processes for entering and reviewing facility data, reviewing relevant guidance, and reviewing written responses CISA officials provided in response to our questions about changes in how CFATS data are stored following the discontinuation of the program. We determined the data to be insufficiently reliable because the data are no longer maintained in a way that reasonably ensures data quality.

We analyzed relevant personnel data from fiscal year 2024 to fiscal year 2025, including the numbers of full-time authorized positions and full-time active personnel. We assessed the reliability of these data by reviewing relevant CISA documents and analyzing written responses CISA officials provided in response to our questions regarding the reliability of the data. We determined that these data were sufficiently reliable for the purpose of identifying changes in CISA personnel levels from fiscal years 2024 to 2025.

We identified and assessed relevant physical and cybersecurity resources available to facility owners and operators from CISA's website, such as ChemLock services and tools, and cybersecurity guidance and resources, such as cyber hygiene guidance and information on ransomware assistance. We also analyzed CISA documents, such as intelligence bulletins and classified reports, and the agency's guidance to critical infrastructure SRMAs for conducting sector risk assessments.

We interviewed CISA officials responsible for leading chemical sector activities on all issues, including the most significant security challenges facing the

chemical sector, the effects of reductions in CISA personnel levels, and steps the agency has taken to meet its SRMA responsibilities, such as the extent to which officials have assessed the feasibility of developing a terrorist vetting program. To better understand how CISA receives intelligence information on sector risks, we interviewed relevant agency officials from DHS's Office of Intelligence and Analysis regarding the collection and sharing of intelligence information.

To obtain private sector stakeholder perspectives, we interviewed representatives from the chemical private sector coordinating council, selected chemical associations, and selected chemical companies. We selected three chemical associations to interview based on: (1) membership in the private sector coordinating council; (2) recommendations from CISA officials and facility owners and operators; and (3) the high-risk chemicals their members manufactured, distributed, or possessed.²⁷

To obtain selected facility owners and operators (companies) perspectives, we interviewed representatives from chemical facilities and their companies, that had experience with the CFATS program. We selected them from the list of approximately 3,200 high-risk chemical facilities that were covered by the CFATS program at the time it was discontinued. From this list, we identified companies with five or more high-risk facilities and companies with one or two high-risk facilities. From among these, we selected companies that met one or more of the following criteria and were willing to meet with us: membership in the private sector coordinating council, facilities in geographic locations near audit team members, or recommended by CISA officials. We interviewed representatives from a total of six chemical companies to better understand the security challenges chemical facility owners and operators face. We interviewed representatives from five companies during site visits to five of their chemical facilities and interviewed representatives from the sixth company by videoconference.²⁸ The testimonial evidence we obtained from association and company interviews is not generalizable to all industry associations and high-risk facility owners and operators but provided us with useful information regarding the perspectives of private sector stakeholders.

We conducted this performance audit from February 2025 through September 2026 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.

Addressee

The Honorable Andrew Garbarino
Chairman
Committee on Homeland Security
House of Representatives

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

For more information, contact: Tina Won Sherman, Director, Homeland Security and Justice, ShermanT@gao.gov.

Public Affairs: Sarah Kaczmarek, Managing Director, media@gao.gov.

Congressional Relations: Dave A. Powner, Acting Managing Director, CongRel@gao.gov.

Staff Acknowledgments: Ben Atwater (Assistant Director), Barbara Guffy (Analyst-in-Charge), Ryan Basen, Ben Crossley, Michele Fejfar, Emilio Fonseca, Tracey King, and Joshua Leiling made key contributions to this report.

Connect with GAO on [Facebook](#), [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).

Visit GAO on the web at <https://www.gao.gov>.

This is a work of the U.S. government but may include copyrighted material. For details, see <https://www.gao.gov/copyright>.

Appendix I: Critical
Infrastructure Sector
Risk Management
Agency (SRMA) Roles
and Responsibilities

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 defines the role of critical infrastructure SRMAs as (1) providing specialized expertise to sector owners and operators, and (2) supporting sector programs and associated activities.²⁹ Table 2 below lists SRMA responsibilities for mitigating security risks to the individual critical infrastructure sectors and the six categories into which they are grouped.

Table 2: Critical Infrastructure Sector Risk Management Agency (SRMA) Responsibilities	
Category of SRMA responsibility	SRMA responsibilities
Support sector risk management	Establish and carry out programs to assist sector owners and operators in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets. Recommend security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets.
Assess sector risk	Identify, assess, and prioritize sector risks, including physical security and cybersecurity threats, vulnerabilities, and consequences. Support DHS national risk assessment efforts.
Sector coordinator	Serve as a day-to-day federal coordinator for the prioritization and coordination of sector activities and responsibilities. Serve as the federal government coordinating council chair for the sector. Participate in cross-sector coordination councils, as appropriate.
Facilitate sharing of information on physical security and cybersecurity threats with DHS and other appropriate federal agencies	Facilitate access to, and exchange of, relevant information and intelligence through information sharing and analysis organizations and the National Cybersecurity and Communications Integration Center. Facilitate the identification of intelligence needs and priorities of sector facility owners and operators, in coordination with the Director of National Intelligence and heads of other Federal departments and agencies, as appropriate. Facilitate awareness within the sector of ongoing and real-time awareness of identified security threats, vulnerabilities, mitigations, and other actions. Support DHS reporting requirements by providing, annually, sector-specific critical infrastructure information.
Support incident management	Support incident management and restoration efforts during or following a security incident.
Contribute to emergency management efforts	Support CISA Director, upon request, in national cybersecurity asset response activities for critical infrastructure. Coordinate with sector owners and operators in the development of planning documents for coordinated action in the event of a national disaster, act of terrorism, or other man-made disaster or emergency. Participate in, conduct or facilitate, exercises and simulations of potential natural disasters, acts of terrorism or other man-made disasters, or emergencies within the sector. Support DHS and other federal departments and agencies in developing sector planning documents or conducting sector exercises or simulations when appropriate.

Source: 6 U.S.C. § 665d. | GAO-26-108127



BY ELECTRONIC SUBMISSION

August 24, 2026

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-108127, "Chemical Security: DHS Should
Provide Options for Voluntary Vetting of Facility Personnel for Terrorist Ties"

Dear Ms. Won Sherman:

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

DHS leadership is pleased to note GAO's positive recognition of the vetting the Cybersecurity and Infrastructure Security Agency (CISA) conducted within the authorities it was previously given under the Chemical Facility Anti-Terrorism Standards (CFATS) Program. Through the CFATS' Personnel Surety Program¹, CISA vetted approximately 500,000 individuals who sought, or had, access to certain chemical facilities, and this resulted in the identification of 13 individuals who were on the U.S. Government's Terrorist Screening Database.

The Department recognizes that efforts to identify and mitigate risks associated with access to chemical facilities are important to protecting critical infrastructure within the chemical sector. However, with the expiration of the statutory authority for the CFATS Program on July 28, 2023, CISA no longer has the statutory and regulatory framework under which the CFATS Program operated, including the requirements established under

¹ The Personnel Surety Program was addressed through Risk-Based Performance Standard (RBPS) 12 under 6 Code of Federal Regulations Part 27.

6 Code of Federal Regulations Part 27. As a result, CISA can no longer require facilities to report their chemicals of interest or submit information through the Chemical Security Assessment Tool, undergo CFATS inspections, or implement CFATS Site Security Plans or CFATS Alternative Security Programs, among other requirements. That said, DHS remains committed to protecting chemical facilities through its role as the Chemical Sector Risk Management Agency, and CISA continues to support the chemical sector security through voluntary resources and services, such as the CISA ChemLock Program.

The draft report contained one recommendation with which the Department non-concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracies, contextual, and other issues under separate **cover for GAO's consideration**, as appropriate.

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,

JEFFREY M BOBICH Digitally signed by JEFFREY M BOBICH
Date: 2026.08.24 11:00:40 -04'00'

JEFFREY M. BOBICH
Executive Director
Financial Management and Systems

**Enclosure: Management Response to Recommendation
Contained in GAO-26-108127**

GAO recommended that the Director of CISA:

Recommendation 1: Identify, evaluate, and implement voluntary options for chemical facility owners and operators to address insider terrorist security risks by vetting their personnel and unescorted visitors with access to restricted areas or critical assets, and, if necessary, seek the legislative authority to do so.

Response: Non-Concur. The voluntary collection and handling of sensitive personal information necessary to conduct such vetting would raise significant legal, privacy, compliance, and resource considerations. These considerations include proper collection, use, maintenance, and protection of sensitive personal information necessary to support such activities, as well as requirements associated with safeguarding personal data and providing appropriate redress.

CISA's Infrastructure Security Division will continue, consistent with its existing authorities, to assist chemical facility owners and operators in addressing personnel-security risks. These efforts, including resources and services provided through the CISA ChemLock Program, will allow CISA to continue working with facilities to defend against **today's threats and collaborate to build a more secure and resilient infrastructure** for the future.

DHS believes these actions are sufficient to meet the intent of the recommendation. Therefore, we request that GAO consider this recommendation closed as implemented.

Accessible Text for Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

BY ELECTRONIC SUBMISSION

August 24, 2026

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-108127, "Chemical Security: DHS Should Provide Options for Voluntary Vetting of Facility Personnel for Terrorist Ties"

Dear Ms. Won Sherman:

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

DHS leadership is pleased to note GAO's positive recognition of the vetting the Cybersecurity and Infrastructure Security Agency (CISA) conducted within the authorities it was previously given under the Chemical Facility Anti-Terrorism Standards (CFATS) Program. Through the CFATS Personnel Surety Program, CISA vetted approximately 500,000 individuals who sought, or had, access to certain chemical facilities, and this resulted in the identification of 13 individuals who were on the U.S. Government's Terrorist Screening Database.

The Department recognizes that efforts to identify and mitigate risks associated with access to chemical facilities are important to protecting critical infrastructure within the chemical sector. However, with the expiration of the statutory authority for the CFATS Program on July 28, 2023, CISA no longer has the statutory and regulatory framework under which the CFATS Program operated, including the requirements established under 6 Code of Federal Regulations Part 27. As a result, CISA can no longer require facilities to report their chemicals of interest or submit information through the Chemical Security Assessment Tool, undergo CFATS inspections, or implement CFATS Site Security Plans or CFATS Alternative Security Programs, among other requirements. That said, DHS remains committed to protecting chemical facilities through its role as the Chemical Sector Risk Management Agency, and CISA continues to support the chemical sector security through voluntary resources and services, such as the CISA ChemLock Program.

¹ The Personnel Surety Program was addressed through Risk-Based Performance Standard (RBPS) 12 under 6 Code of Federal Regulations Part 27.

The draft report contained one recommendation with which the Department non-concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracies, contextual, and other issues under separate cover for GAO's consideration, as appropriate.

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,

JEFFREY M. BOBICH
Executive Director
Financial Management and Systems

**Enclosure: Management Response to Recommendation
Contained in GAO-26-108127**

GAO recommended that the Director of CISA:

Recommendation 1: Identify, evaluate, and implement voluntary options for chemical facility owners and operators to address insider terrorist security risks by vetting their personnel and unescorted visitors with access to restricted areas or critical assets, and, if necessary, seek the legislative authority to do so.

Response: Non-Concur. The voluntary collection and handling of sensitive personal information necessary to conduct such vetting would raise significant legal, privacy, compliance, and resource considerations. These considerations include proper collection, use, maintenance, and protection of sensitive personal information necessary to support such activities, as well as requirements associated with safeguarding personal data and providing appropriate redress.

CISA's Infrastructure Security Division will continue, consistent with its existing authorities, to assist chemical facility owners and operators in addressing personnel-security risks. These efforts, including resources and services provided through the CISA ChemLock Program, will allow CISA to continue working with facilities to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.

DHS believes these actions are sufficient to meet the intent of the recommendation. Therefore, we request that GAO consider this recommendation closed as implemented.

Endnotes

¹6 U.S.C. § 652(c)(4).

²6 U.S.C. § 101(4). The critical infrastructure sectors were most recently defined in *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), which as of June 2026 was under review pursuant to Executive Order 14239. Exec. Order No. 14239, 90 Fed. Reg. 13267 (Mar. 21, 2025).

³6 U.S.C. § 665d.

⁴The sector government coordinating council—known as the “government coordinating council” or GCC—is the government counterpart of the private sector coordinating council—known as the “sector coordinating council,” or SCC. It is comprised of representatives from across various levels of government (federal, state, local, tribal, and territorial), as appropriate, and is chaired by a representative from CISA (as the SRMA). Its purpose is to ensure appropriate representation on the council and provide cross-sector coordination with state, local, tribal, and territorial governments.

⁵The CFATS program was first established pursuant to the DHS appropriations act for fiscal year 2007, which required DHS to issue regulations to establish risk-based performance standards for securing high-risk chemical facilities. Pub. L. No. 109-295, § 550, 120 Stat. 1355, 1388 (2006).

⁶Appendix A of the CFATS regulations lists more than 300 “chemicals of interest.” The chemicals were categorized according to three main security issues: release, theft or diversion, and sabotage. They included chemicals that are toxic, flammable, explosive (and their precursors), chemical warfare agents (and their precursors), and those that are water reactive. Facility owners and operators that possessed or planned to possess these chemicals, in the designated threshold quantities, were required to provide information to CISA about their facilities, which CISA used to determine if the facilities were “high risk.” Certain facilities that might otherwise have qualified for CFATS were excluded by statute. These included, but were not limited to, facilities regulated under the Maritime Transportation Security Act (33 C.F.R. Part 105); public water systems, as defined in 42 U.S.C. § 300; treatment works, as defined in 33 U.S.C. § 1292; and facilities owned or operated by the Department of Defense or Energy. 6 C.F.R. pt. 27.

⁷Other key actions CISA took through the CFATS program included training facility personnel about information that related to vulnerabilities of high-risk chemical facilities and how to protect that information from disclosure and collecting Security Vulnerability Assessments from high-risk facilities.

⁸Individuals seeking unescorted access to restricted areas of a chemical facility or critical assets could include contractors and other service personnel.

⁹According to CISA officials, there was a regular flow of names submitted and removed from the direct vetting option under the Personnel Surety Program. Officials stated that the total number of individuals vetted in the first half of 2023—the CFATS program was discontinued in July 2023—was fairly consistent with the number of individuals vetted throughout the program’s existence.

¹⁰The “terrorist watchlist” is an unclassified dataset of individuals the U.S. government has identified as having a nexus to terrorism. The watchlist is managed by the FBI’s Threat Screening Center and is derived from a classified database containing biographic (e.g., first and last names and date of birth) and biometric (e.g., photographs and fingerprints) identifying information. As appropriate, the FBI and DHS share terrorist watchlist records with federal government agencies and other government entities that have arrangements to share terrorist vetting information for homeland security, law enforcement, and other authorized functions.

¹¹The chemical associations and the chemical companies we interviewed had direct experience with the Personnel Surety Program because they owned or operated high-risk facilities covered by CFATS during the program’s operations.

¹²In 2013, we reported on the challenges DHS had faced in determining how to implement the terrorist vetting requirements of the CFATS program. GAO, *Critical Infrastructure Protection: DHS Efforts to Assess Chemical Security Risk and Gather Feedback on Facility Outreach Can Be Strengthened*, [GAO-13-353](#) (Washington, D.C.: April 5, 2013).

¹³CISA implemented the Personnel Surety Program in two stages. The first stage was implemented in December 2015, for high-risk chemical facilities CISA deemed at greatest risk. In July 2019, CISA implemented terrorist vetting for all CFATS-covered facilities.

¹⁴Other DHS programs included the Hazardous Materials Endorsement Program, Secure Electronic Network for Travelers Rapid Inspection, and Free and Secure Trade. Each of these DHS programs conducts continuous vetting.

¹⁵CISA noted that Option 4 provided a more limited security benefit, as visual inspection may make it more difficult to ascertain whether a credential has expired, been revoked, or is fraudulent. 80 Fed. Reg. 79058, 79063 (Dec. 18, 2015).

¹⁶William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002(c)(1), 134 Stat. 3388, 4770-73 (2021) (codified as amended at 6 U.S.C. § 665d). As shown in Appendix I, CISA, as SRMA, is responsible for establishing and carrying out programs to assist chemical sector owners and operators in identifying and mitigating threats and vulnerabilities.

¹⁷CISA officials told us they provide incident-response services through their headquarters-based response team. Due to resource constraints, CISA prioritizes the services of this team to significant incidents with widespread consequences.

¹⁸“Authorized positions” refers to the total number of positions authorized in CISA’s annual budget.

¹⁹Since January 2025, the Executive Branch has taken several steps to reduce the size of its workforce. Both the Office of Personnel Management and DHS have offered deferred resignation programs to eligible employees. Full-time permanent and Senior Executive Service employees were eligible for both programs. DHS also offered Voluntary Early Retirement Authority and Voluntary Separation Incentive Payment for eligible employees. We have issued reports examining workforce reductions since January 2025 at DHS and other federal agencies. See GAO, *Federal Agency Workforce Changes: Update for January to June 2025*, [GAO-26-108719](#) (Washington, D.C.: Feb. 24, 2026) and *Federal Agency Workforce Changes: Update for July 2025 to January 2026*, [GAO-26-108583](#) (Washington, D.C.: Jun. 17, 2026).

²⁰DHS’s Countering Weapons of Mass Destruction Office issued the *Department of Homeland Security Chemical Defense Strategy* in December 2019 and updated it in 2021 with an implementation plan. This strategy was designed to enable an integrated and coordinated departmental approach to preventing chemical attacks and preparing for chemical attacks and related incidents. See Department of Homeland Security Chemical Defense Strategy (Washington, D.C.: Dec. 20, 2019). The explanatory statement accompanying the Consolidated Appropriations Act, 2026, provided that certain functions of the Countering Weapons of Mass Destruction Office were to be moved to other offices. Explanatory statement accompanying H.R. 7147, Department of Homeland Security Appropriations Act, 2026, 172 Cong. Rec. H1664 (2026). The Homeland Security and Further Additional Continuing Appropriations Act, 2026, provided that most sections of the explanatory statement accompanying H.R. 7147 were to have the same effect as if the explanatory statement were a joint explanatory statement of a conference committee. Pub. L. No. 119-86, § 4, 140 Stat. 773 (2026).

²¹The National Security Council is the President’s principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinets officials.

²²DHS, CISA, *Sector-Specific Risk Assessment Guide*, v. 1.1 (June 14, 2024).

²³These seven risk scenarios involved cyber incidents, physical incidents, natural hazards, and supply chain disruptions.

²⁴The *National Security Memorandum on Critical Infrastructure Security and Resilience/NSM-22*, issued on April 30, 2024, directed critical infrastructure SRMAs, including CISA as SRMA for the chemical sector, to, among other tasks, develop sector risk assessments and management plans for addressing those risks.

²⁵According to CISA, pursuant to Executive Order 14239, policies such as the *National Security Memorandum on Critical Infrastructure Security and Resilience/NSM-22* and related deliverables are under review, as of May 2026. Executive Order 14239, issued on March 21, 2025, directs the Assistant to the President for National Security Affairs, in coordination with the Director of the Office of Science and Technology Policy and the heads of relevant agencies, to review, within 180 days of the issuance of the order, all critical infrastructure policies and recommend to the President the revisions, rescissions, and replacements necessary to achieve a more resilient posture, shift from an

all-hazards approach to a risk-informed approach, and move beyond information sharing to action. Exec. Order No. 14239, 90 Fed. Reg. 13267 (Mar 21, 2025).

²⁶6 U.S.C. § 665d. The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience: National Security Memorandum/NSM-22* (Washington, D.C.: April 30, 2024).

²⁷American Chemistry Council; Alliance for Chemical Distribution; and American Fuel & Petrochemical Manufacturers.

²⁸We interviewed representative from the following six companies: Baltimore Gas and Electric Company; Brenntag North America LLC; CF Industries Holdings, Inc.; Energy Transfer LP; Nutrien Ltd; and Tilley Distribution Inc.

²⁹William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002(c)(1), 134 Stat. 3388, 4770-73 (2021) (codified as amended at 6 U.S.C. § 665d).