IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Chemical Facility Anti-Terrorism Standards: Authorization Inspections

Overview

The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) program works with facilities to ensure security measures are in place to reduce the risk of certain hazardous chemicals being weaponized. High-risk facilities are assigned to one of four risk-based tiers and must develop a security plan tailored to the tier level and unique circumstances. The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (6 U.S.C. § 621, et seq.) and the CFATS regulation (6 CFR Part 27) provide CISA the authority to enter, inspect, and audit the property, equipment, operations, and records of CFATS-covered facilities.

Authorization Inspection (AI) Overview

CISA requires facilities determined to be high-risk to develop and implement one of two types of security plans: a Site Security Plan (SSP) or an Alternative Security Program (ASP).[1] After a facility submits the SSP/ASP for review, CISA Chemical Security Inspectors (CSIs) conduct an Authorization Inspection, or AI, at the facility to verify and validate that the content listed in the facility's security plan is accurate and complete, and to assist the facility in resolving any identified potential gaps. For the SSP/ASP to be approved, the facility's existing and planned equipment, processes, and procedures must sufficiently meet CISA's risk-based performance standards (RBPS).

Notification and Preparation for an AI

To notify a facility of an AI, CISA sends the facility a Letter of Authorization via the Chemical Security Assessment Tool (CSAT)—the online portal for chemical facilities and CISA to submit and receive information. In addition, a CISA Inspector contacts the facility site representative by phone and/or email to schedule a date and time for the AI.

What Is the AI Process?

During the Inspection

The CISA inspection team will conduct a briefing that will cover the purpose and intent of the inspection, Chemical-terrorism Vulnerability Information (CVI) authorized user status for all personnel present, and personal protective equipment/safety requirements.

The inspection team will evaluate the facility's security measures through direct observation, document review, equipment testing, and interviews.

---

[1] Tier 3 and 4 facilities also have the option to submit a security plan under the Expedited Approval Program (EAP). This process removes the AI requirement. Facilities that choose this option must follow the prescriptive security measures (6 U.S.C. § 622(c)(4)(B)(i)) in the CISA EAP Guidance to satisfy the RBPS. Visit cisa.gov/cfats-expedited-approval-program for more information.

A facility may want to make the following documents available for review during a AI:

- All CFATS-related documents and correspondence
- Chemical inventory list
- Company hiring policy and procedures
- Crisis Management Plan (or equivalent)
- Cybersecurity policy and procedures
- Security standard operation procedure (SOP)
- Incidents and breaches of security documentation
- Security system maintenance/calibration records
- Shipping and receiving policies and procedures
- Site/facility layout
- Training, drill, and exercise records

Appropriate personnel should be available during the AI to be interviewed, such as the CSAT submitter, authorizer, and preparer; the facility security officer; cybersecurity officer; human resources representative; and operations manager. It is not necessary for all personnel to be present for the entirety of the inspection, and the inspection team may be able to conduct phone interviews with individuals that are unavailable in person.

Additionally, the inspection team will verify the facility's COI inventory against the latest submitted Top-Screen. If inaccuracies are found, the facility will be required to resubmit a Top-Screen with the correct COI information.

After the Inspection

The inspection team will provide an overview of the observations, findings, and potential concerns, and discuss follow-up actions. The SSP/ASP may be edited while the inspection team is onsite to assist in updates and to address any inspection findings. After review of the resubmitted SSP/ASP, information gathered during the inspection, and other relevant information, CISA will take one of two actions:

- If the review of all information and analysis indicates that the SSP/ASP meets the CFATS requirements, CISA will approve the SSP/ASP and issue a Letter of Approval to the facility. Upon receiving a Letter of Approval, the facility must implement the approved SSP/ASP.
- In the event that a review of the inspection data or other information indicates that the SSP/ASP fails to meet the CFATS requirements, CISA will notify the facility in writing of the deficiencies in the security plan. The facility must then resubmit an SSP/ASP addressing those deficiencies by a specified date.

Tools and Resources

After a facility's security plan is approved, the facility will receive a Letter of Approval and enter the CFATS compliance cycle, which includes regular and reoccurring Compliance Inspections (CI).

- CFATS Resources: cisa.gov/cfats-resources
- CFATS Process: cisa.gov/cfats-process
- RBPS Guidance: cisa.gov/publication/cfats-rbps-guidance
- CSAT SSP Submission Tips: cisa.gov/csat-ssp-submission-tips
- Request a Compliance Assistance Visit: cisa.gov/request-compliance-assistance-visit
- CVI: cisa.gov/chemical-terrorism-vulnerability-information
- CFATS Expedited Approval Program (EAP) for Tier 3 and 4 facilities: cisa.gov/cfats-expedited-approval-program
- CFATS Knowledge Center: csat-help.dhs.gov
- CSAT Help Desk (technical assistance): Call 1-866-323-2957 or email csat@hq.dhs.gov