Chemical Facility Anti-Terrorism Standards: Compliance Inspection (CI)

The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) program works with facilities to ensure they have security measures in place to reduce the risk of certain hazardous chemicals from being weaponized. High-risk facilities are assigned to one of four risk-based tiers and must develop a security plan tailored to their 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.

Compliance Inspection (CI) Overview

Under CFATS, 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 either the SSP or ASP for review, CISA inspectors conduct an Authorization Inspection (AI) at the facility to verify that the content listed in the facility's security plan is accurate and complete. After the facility's SSP or ASP is approved, they receive a Letter of Approval and enter into the CFATS compliance cycle, which includes regular and reoccurring CIs.

A CI is conducted by CISA Chemical Security Inspectors (CSI) to verify that the equipment, processes, and procedures described in the facility's approved SSP or ASP have been implemented and continue to sufficiently meet CISA's risk-based performance standards (RBPS), and that any required corrective actions have been implemented and are sustainable. A CI can also be conducted to discuss issues raised by CISA after a review of the facility's case file.

Notification and Preparing for a CI

To notify a facility of a CI, CISA sends the facility a Notice of Inspection via the Chemical Security Assessment Tool (CSAT). In addition, a CISA inspector contacts the facility site representative by phone and/or email to schedule a date and time. Except in exigent circumstances, CISA will provide at least a 24-hour notice.

The best way to prepare for a CI is to conduct the required annual audit of the SSP/ASP. During this audit, the facility should review all existing and planned measures within the SSP/ASP; identify all policies, procedures, and records within the SSP/ASP; review the facility's inventory compared against the latest Top-Screen; and be prepared to demonstrate and present these to the CISA Inspector.

---

[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.

What Is the CI Process?

During the Inspection

The CISA inspection team will conduct an in-brief that will cover the purpose and intent of the inspection, review Chemical-terrorism Vulnerability Information (CVI) authorized user status for all personnel present, and any necessary safety instructions that may be required.

The inspection team will review and verify existing security measures, the stage of implementation and effectiveness of planned measures, and significant changes in the security posture since the last inspection through direct observation, document review, equipment testing, and interviews.

A facility may want to have the following documents readily available for review during the CI:

- All CFATS-related documents and correspondence
- Chemical inventory list
- Company hiring policy and procedures
- Crisis Management Plan (or equivalent)
- Cybersecurity policy and procedures
- Documents describing the progress or completion of planned measures
- Incidents and breaches of security documentation
- Procedures and records pertaining to the shipping, receiving, storage, and transportation of chemicals
- Records for RBPS 18
- Security standard operation procedure (SOP)
- Security system maintenance/ calibration records
- Site/facility layout

Appropriate personnel should be available during the CI to be interviewed, such as the CSAT submitter, authorizer, and preparer; 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 CI.

After the Inspection

The inspection team will conduct an out-brief of the results, potential concerns, and/or infractions.

- If no issues are raised by the CI, the facility will receive a "Post-Compliance Inspection Status" letter for their continued compliance.
- If issues are raised by the CI, the facility may need to edit and resubmit their SSP/ASP or correct infractions based on the inspection team's findings.

Tools and Resources

- CFATS Resources: www.cisa.gov/cfats-resources
- CFATS Process: www.cisa.gov/cfats-process
- RBPS Guidance: www.cisa.gov/publication/cfats-rbps-guidance
- RBPS 18 – Records: www.cisa.gov/rbps-18-records
- CFATS SSP Submission Tips: www.cisa.gov/csat-ssp-submission-tips
- Request a Compliance Assistance Visit: www.cisa.gov/request-compliance-assistance-visit
- CVI: www.cisa.gov/chemical-terrorism-vulnerability-information
- CFATS Expedited Approval Program (EAP) Guidance (for Tier 3 and 4 facilities): www.cisa.gov/publication/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

Contact Information

For any questions or comments, email CFATS@hq.dhs.gov or visit www.cisa.gov/cfats.