The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

What to Expect from a CFATS Authorization Inspection

Homeland Security

What is an Authorization Inspection?

- A CFATS **Authorization Inspection (AI)** is conducted at covered facilities to verify and validate that the content listed in the facility's authorized Site Security Plan (SSP) or Alternative Security Program (ASP) is accurate and complete and that existing and planned equipment, processes, and procedures are appropriate and sufficient to meet the established Risk-Based Performance Standards (RBPS) requirements.
- Section 550 of the Homeland Security Appropriations Act of 2007 and CFATS, 6 C.F.R. Part 27 provide the authority for DHS to conduct authorization inspections
  - Section 550(e) provides authority for "[t]he Secretary…to audit and inspect chemical facilities for the purposes of determining compliance with [the requirements under CFATS]." Public Law 109-295, Section 550.
  - Section 27.250 of CFATS authorizes Department of Homeland Security (DHS) inspectors to enter, inspect, and audit the property, equipment, operations, and records of covered facilities.

Homeland Security

Before an Inspection

- When your facility is ready for an Authorization Inspection, it will receive a Letter of Authorization from DHS. In addition, an inspector will reach out by phone and/or email to the designated site representative to schedule a date and time for the AI.
- The inspector will discuss the:
  - Purpose and scope of the visit
  - Expected duration and schedule of the inspection
  - Required facility personnel and resources/documents that should be available during the inspection
  - Chemical-terrorism Vulnerability Information (CVI) considerations
  - Personal protective equipment/safety requirements

Homeland Security

Preparation for the Inspection Team: Pre-Arrival

- What are examples of items my facility may want to have on hand?
  - Chemical inventory list
  - Site/facility layout
  - CFATS-related documents and correspondence (SSP, SVA, TS, FTL, Notice of Inspection, etc.)
  - Security SOP
  - Crisis Management Plan (or equivalent)
  - Cybersecurity policy and procedures
  - Company hiring policy and procedures
  - Shipping and receiving policy and procedures
  - Training, drill, and exercise records
  - Security system maintenance/calibration records
  - Incidents and breaches of security documentation

Note: Facilities may choose to have either electronic or hard copies available.

Homeland Security

Who should be present on site or available during the inspection?

- Not all personnel need to be present for the entirety, but you should consider whether to include:
  - Submitter/Authorizer/Preparer(s) of the security plan
  - Facility Security Officer and/or Corporate Security Officer
  - Cybersecurity Officer
  - Human Resources representative
  - Facility Manager
  - Facility security representative
  - Operations Manager
  - Shipping and Receiving representative
  - Emergency Response representative
  - Rail Services representative

The Inspection

- The inspection team will arrive early enough to allow time for security and/or safety briefings and will conduct an inbrief to discuss the purpose of the visit and planned schedule for the inspection.
- The facility's SSP or ASP will be opened at the beginning of the inspection so that the facility can update the SSP/ASP with the inspection team onsite and can resubmit to address any inspection findings.
- During the inspection, there are four distinct methods of collecting information when evaluating a security measure:
  - Direct observation
  - Document review
  - Testing
  - Interviews

Homeland Security

During the Inspection

- Direct Observation:
  - Observing persons, places, operations, or systems allows inspectors to obtain a general picture of the security measures to verify compliance
- Document Review:
  - The inspectors can review all relevant records or documents associated with the facility's compliance with the SSP/ASP
- Testing:
  - Testing encompasses those procedures used to assess the performance of security equipment, processes, or procedures
- Interviews:
  - Inspectors may conduct formal and informal discussions with facility and/or corporate personnel regarding the verification of security measures, policies, and procedures

Inspection Outbrief

- During the outbrief, the inspection team will:
  - Provide a general overview of the just conducted inspection
  - Relay observations, findings, and potential concerns encountered
  - Present observations to clarify any misunderstandings and/or provide clarifying documentation
  - Discuss follow-up actions or next steps with the facility

Homeland Security

Post-inspection

- The facility's security plan will remain open for 30 days from the start of the inspection to permit the facility to make any changes discussed during the inspection.
- After review of the updated SSP/ASP and the inspection team's report, DHS will take one of the following actions:
  - If all information and analysis indicates that the SSP meets the requirements of CFATS, DHS will approve your facility's SSP and issue a Letter of Approval to the facility. Please be aware the facility will be subject to future compliance inspections after receipt of the Letter of Approval.
  - In the event that a review of the inspection data or other information indicates that the SSP fails to meet the requirements of CFATS, DHS will notify the facility of the deficiencies in the SSP. The facility must then resubmit a sufficient SSP addressing those deficiencies by a specified date. If the facility fails to address the deficiencies, DHS may disapprove the facility's security plan.

Homeland Security

SSP Lessons Learned

- When updating the SSP, below are some best practices to consider:
  - Include information on all applicable Risk-Based Performance Standards (RBPS). To simplify, there are five security areas a facility should consider when completing the SSP/ASP: Detection, Delay, Response/Mitigation, Security Management, and Cybersecurity.
  - Include detailed descriptions of security measures within the “other” boxes.
  - Think about safety or engineering items that your facility could use as a security feature.
  - Facilities that identify assets need to define the assets in the asset-specific section and describe the associated security measures in detail.
  - All planned measures need to include an implementation timeline and specific detail regarding what the planned measure includes.

SSP Lessons Learned (cont.)

- Below are a few RBPS-specific best practices to consider:
  - RBPS 8 – Cyber: Facilities should seek to identify the types of systems that impact the security of their Chemicals of Interest (COI) and focus on the security measures in place to protect these systems.
  - RBPS 12 – Personnel Surety: Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets.
  - RBPS 18 – Records: Addresses the creation, maintenance, protection, storage, and disposal of appropriate security-related records pursuant to 6 CFR § 27.255. Facilities cannot be approved without acknowledging in the SSP/ASP that all the records will be stored and maintained per the regulation.

Resources

- To familiarize staff with the CFATS Compliance process and requirements, we recommend the following resources:
  - DHS Chemical Security Website: http://www.dhs.gov/critical-infrastructure-chemical-security
  - Risk Based Performance Standards (RBPS) document: http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf
  - DHS Web based Security Awareness Training Website: http://www.dhs.gov/chemical-sector-training-and-resources
  - Chemical Vulnerability Information (CVI) Training: http://www.dhs.gov/training-chemical-terrorism-vulnerability-information
  - DHS Cyber Resource: http://ics-cert.us-cert.gov/ics-cert
  - National Terrorism Advisory System (NTAS): http://www.dhs.gov/national-terrorism-advisory-system

Homeland Security

Homeland Security

For more information, visit:
www.dhs.gov/critical-infrastructure

CFATS Knowledge Center

866-323-2957

http://csat-help.dhs.gov