



Homeland Security

What to Expect from a CFATS Authorization Inspection

What is an Authorization Inspection?

Under the Chemical Facility Anti-Terrorism Standards (CFATS), an 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.

Both Section 550 of the Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 § 550 (2006), and CFATS, 6 C.F.R. Part 27, provide authority for DHS to conduct authorization inspections. Specifically, 6 C.F.R. § 27.250(a) provides authority for the Department of Homeland Security (DHS or the Department) to enter, inspect, and audit the property, equipment, operations, and records of CFATS covered facilities.

When DHS determines that a facility is ready for an AI, DHS will send the facility a Letter of Authorization through CSAT. In addition, an inspector will reach out by phone and/or email to the designated facility site representative to schedule a date and time for the AI. During the AI, the inspector will discuss the following topics:

- 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 requirement

What should a facility do to prepare for an Authorization Inspection?

A facility may want to have readily available a chemical inventory list, a site/facility layout map, all CFATS-related documents required under 6 C.F.R. § 27.255 (Recordkeeping Requirements), and all procedures and records pertaining to the storage and transportation of chemicals.

Key personnel should be available during the AI, such as, the facility manager and facility security representative, operations manager, and the submitter of the security plan.

What occurs during and after the Authorization Inspection?

The inspection team will participate in any security or safety briefings and will conduct an in-brief to discuss the purpose of the AI and the planned schedule for the inspection. The Facility's SSP or ASP will be opened at the beginning of the AI so that the facility can update the SSP/ASP with the inspection team onsite.



After the inspection is complete, the inspection team will provide an out-brief for the facility to provide a general overview of the issues raised by the AI and discuss next steps.

The facility's security plan will remain open for 30 days post-AI to permit the facility to make any changes. Once submitted, DHS will review the updated SSP/ASP, the authorization inspection report, and any other relevant information and determine whether to approve the facility's security plan. If DHS finds that all applicable RBPSs are sufficient, DHS will send the facility a Letter of Approval through CSAT. DHS will then conduct periodic compliance inspections and audits of the facility to ensure continued compliance with the facility's approved security plan. If DHS finds that all applicable RBPSs in the facility's security plan are not sufficient, DHS will send the facility a Notice of Deficiency through CSAT as required by 6 C.F.R. § 27.245(b). The facility must then resubmit a sufficient security plan addressing the deficiencies by a specific date. If the resubmitted security plan does not satisfy the requirements of 6 C.F.R. § 27.225, then DHS may disapprove the facility's security plan.

SSP Lessons Learned

When updating the SSP, a facility may choose to consider the following best practices:

- Include information on all applicable RBPSs. 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 take an asset-based approach to security should 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.

A few RBPS-specific best practices to consider include:

- RBPS 8 – Cyber: Facilities should 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: Section 27.255 of CFATS sets out the records a covered facility must keep and for what time period. A facility security plan should include language stating that it will maintain all of the records required by 6 C.F.R. 27.255.

Contact Information

To learn more about CFATS and Chemical Security Inspectors, visit: <http://www.dhs.gov/critical-infrastructure-chemical-security>.

To ask a Department representative to speak on the CFATS regulatory program, please contact cfats@hq.dhs.gov.

Reporting Potential CFATS Concerns

To report a possible security concern involving the CFATS regulation, call the Tip Line at **877-394-4347** (877-FYI 4 DHS). Calls to this tip line should involve the CFATS regulation at your facility or another facility. You may report concerns on voicemail anonymously. To receive a return call, leave your name and number.

If you have a security emergency or terrorist incident, call 911 or contact your local FBI field office.