CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS): WHAT TO EXPECT DURING A CFATS INSPECTION

CISA
CYBER+INFRASTRUCTURE

Chris McNeely & Doug Frey July 2019

CFATS Inspections

Chemical Security Inspectors conduct several types of inspections and visits to facilities, including:

- **Compliance Assistance Visits**: Conducted at any stage of CFATS implementation to provide technical assistance and educate covered facilities on the CFATS regulation
- **Authorization Inspections**: Conducted at a covered facility after a Letter of Authorization in order to verify that the contents listed in the facility's authorized Site Security Plan (SSP) or Alternative Security Program (ASP) are accurate and complete, and that the equipment, processes, and procedures described are appropriate and sufficient to meet applicable performance standards
- **Compliance Inspections**: Conducted after a Letter of Approval to ensure both existing and planned security measures that are identified within the approved SSP or ASP continue to be implemented fully and on schedule

What Is an Authorization Inspection?

An **Authorization Inspection (AI)** is conducted at a covered facility after a Letter of Authorization in order to verify that the contents listed in the facility's authorized Site Security Plan (SSP) or Alternative Security Program (ASP) are accurate and complete.

- **AIs are conducted to:**
  - Ensure both existing and planned security measures that are identified within the Authorized SSP or ASP are accurate and complete
  - Ensure that the equipment, processes, and procedures described in the SSP or ASP are appropriate and sufficient to meet the established performance standards
  - Discuss other issues that have come up since the *Letter of Authorization*

What Is a Compliance Inspection?

A **Compliance Inspection (CI)** is conducted as part of the recurring inspection process after a *Letter of Approval* has been issued to ensure the facility continues to implement its approved security plan

- **Compliance Inspections are conducted:**
  - To ensure that both existing and planned security measures that are identified in the approved SSP or ASP continue to be implemented fully and on schedule
  - To ensure that the equipment, processes, and procedures described in the SSP or ASP meet the established risk-based performance standards
  - To ensure that required corrective actions have been implemented and are sustainable
  - To discuss other issues that have come up since the Letter of Approval

CISA
CYBER+INFRASTRUCTURE

Before an Inspection

- An AI/CI will be initiated after a facility has received a Letter of Authorization / Approval from DHS. CI initiation also uses eight prioritization factors developed by DHS.
- An inspector will reach out by phone and / or email to the designated site representative to schedule a date and time for the inspection.
- 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

CISA
CYBER+INFRASTRUCTURE

During an Inspection

Who should be present from the facility during an inspection?

- Not all personnel need to be present for the entirety of the inspection or available in person, 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

Preparing for a CFATS Inspection

- The best way to prepare for your AI/CI is to review your Top-Screen, Security Vulnerability Assessment (SVA), and SSP/ASP
- This review can coincide with the required annual audit
- Review the Top-Screen to:
  - Confirm the current quantities, concentrations, packaging, etc., of all chemicals of interest (COI)
- Review the SVA and SSP/ASP to:
  - Confirm all existing measures are in place and identify methods to demonstrate their effectiveness to the inspection team (e.g., observation, documentation, interview, and testing)
  - Identify all planned measures, ensure their completion on time, and identify methods to demonstrate their effectiveness to the inspection team
  - Identify any changes in the overall security posture of the facility

Demonstrating Existing Measures

- Inspectors will observe security measures as appropriate, but what items should your facility have on hand to demonstrate existing measures?

- Chemical inventory list
- Site/facility layout
- Security Standard Operating Procedures
- 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
- CFATS SSP/ASP annual audit documentation

Demonstrating Planned Measures

- Inspectors will observe completed planned measures, but will also request documentation demonstrating the completion of planned measures and the dates they were completed:
  - Policies/procedures
  - Revised schematics
  - Requests for quotes/proposals
  - Statements of work
  - Budget approval documentation
  - Installation or maintenance records

How to Handle Changes

- Your facility must submit revised Top-Screens within 60 days of a material modification
- Your facility must continue to implement the approved SSP/ASP unless a revision is approved
- If your facility identifies a change in COI:
  - Submit a revised Top-Screen
  - Contact the inspection team
- If your facility identifies a change in an existing security measure:
  - Identify why the change occurred and if the change was in error or is a proposed change to the security posture
  - Determine the resolution to the change
    - ❑ Correct the change and return to the previous security posture or
    - ❑ Ensure the change provides an equivalent level of security to the previous measure and propose the new measure via a resubmitted SSP/ASP
  - Contact the inspection team

How to Handle Delayed Planned Measures

- Your facility must implement all planned measures on time to stay in compliance

- If your facility identified a planned measure that will not be completed on time:
  - Identify why the planned measure was not completed
  - Attempt to correct the issue as quickly as possible
  - Identify and implement compensatory measures, if applicable
  - Notify the inspection team and propose a new completion timeframe

CISA
CYBER+INFRASTRUCTURE

Expediting on the Onsite Visit

- In order to expedite the onsite visit, the inspection team will review your entire case file and determine if certain aspects of your security plan can be verified beforehand
- The inspector(s) may request documentation or conduct phone interviews to verify items such as:
  - Cyber systems and their integration to the security of your COI
  - Response plans and outreach with first responders
  - Security Awareness and Training Program
  - Background checks
  - Elevated and specific threat planning
  - Incident reporting and investigations
  - Security organization
  - Recordkeeping

Onsite Inspection

- The inspection team will arrive early enough to allow time for security and/or safety briefings and will conduct an in-brief to discuss the purpose of the visit and planned schedule for the inspection

- The facility's SSP/ASP will only be opened during a CI if the inspection team deems edits necessary

- During the inspection, there are four distinct methods of collecting information when evaluating a security measure:
  - Direct observation
  - Document review
  - Testing
  - Interviews

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 Out-Brief

- During the out-brief, the inspection team will:
  - Provide a general overview of the 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
- If necessary, the inspection team may leave the facility with a "leave behind" document which outlines the inspection findings and options for consideration in resolving issues

Post-Authorization Inspection

- The facility will have 30 days from the date of the AI to complete any edits necessary to the SSP / ASP.
- After review of the inspection team’s reports and the facility’s edited SSP / ASP DHS will determine if the facility’s SSP / ASP is approved.
- If the facility SSP / ASP is approved, DHS will issue the facility a “Letter of Approval.”
- The Letter of Approval directs the facility to implement the facility's SSP / ASP. The date of approval also starts the clock on any planned measures the SSP / ASP has defined.

Post-Compliance Inspection

- After review of the inspection team’s report, DHS will determine if the facility remains in compliance with their approved SSP/ASP
- If the facility remains in compliance, DHS will issue the facility a “Post-Compliance Inspection Status” Letter
- If the facility is found not to be in compliance, this may trigger potential an enforcement action, such as:
  - Failure to Allow Inspection (6 C.F.R. § 27.250)
  - Security Measures Not Implemented in Accordance with Site Security Plan (6 C.F.R. § 27.225) or Alternative Security Program (6 C.F.R. § 27.235)
  - Maintenance of Records (6 C.F.R. § 27.255)
  - Improper Handling/Disclosure of CVI (6 C.F.R. § 27.400(d))

Compliance Inspections 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:

- https://www.dhs.gov/publication/cfats-rbps-guidance

DHS Web-Based Security Awareness Training Website:

- https://www.dhs.gov/cisa/chemical-sector-training

Chemical Vulnerability Information (CVI) Training:

- https://www.dhs.gov/cisa/cvi-authorized-user-training

DHS Cyber Resource:

- https://www.us-cert.gov/

National Terrorism Advisory System (NTAS):

- http://www.dhs.gov/national-terrorism-advisory-system

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE