# CFATS Risk-Based Performance Standard (RBPS) 9 – Response



## Overview

The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and works with high-risk facilities to ensure security measures are in place to reduce the risk of more than 300 chemicals of interest (COI) being weaponized. High-risk facilities are assigned to one of four risk-based tiers and must develop a security plan meeting the 18 risk-based performance standards (RBPS) criteria. Facilities have flexibility to select measures tailored to the tier level and unique circumstances.

## RBPS 9 – Response at a Glance

**RBPS 9 – Response is the performance standard to develop and exercise emergency plans in response to security incidents at the facility with the assistance of local law enforcement and first responders.**

Planning and training are important to ensure that facility personnel, onsite security, law enforcement, and first responders can effectively respond to external and internal security incidents in a timely manner. These incidents include the theft or diversion of a COI; an onsite fire, explosion, or release of a COI; and loss of containment of a COI.

Examples of security measures include identifying hazards, planning an effective response, identifying the number of responders and the response skills needed for different types of adversary events, and equipping and training response personnel in order to maximize their efficiency and knowledge of a site.

## Security Response vs. Emergency Response

It is important not to confuse a "security response," which is intended to engage and neutralize adversaries, with the broader "emergency response," which follows an attack and attempts to reduce the severity of the event. The initial "security response" has tactical considerations, whereas the "emergency response" relates to containing the damage and mitigating the consequences of a security incident. CFATS-covered facilities should address both responses in planning.

## Security Measures for Response

Properly trained and equipped personnel coupled with well-thought-out and rehearsed plans can reduce the probability of an attack achieving the adversaries' desired goals.

### Crisis Management Plan

A comprehensive crisis management plan should contain response strategies for different types of security incidents, such as:

- Contingency plans
- Emergency response
- Evacuation
- Notification control
- Post-incident security (e.g., post-terrorist attack, accident, or natural disaster)
- Security Response

Crisis management plans generally contain documented agreements with offsite responders, including:

- Ambulance/medical support
- Environmental restoration support
- Explosive device disposal support
- Firefighting support
- Hazardous spill/recovery support
- Marine support

### Drills, Trainings, and Exercises

Drills, trainings, and exercises (e.g., tabletop and full-scale exercises) play a vital role in maximizing and testing the efficiency of the response plan to a security incident, as well as addressing any identified vulnerabilities. Involving local first responders when preparing the plan and conducting drills can carry significant benefits for the facility. The first time that local law enforcement or responders actually access the facility should not be the day of an incident.

## Involving Local Law Enforcement and First Responders

RBPS 9 requires that facilities are capable of responding to incidents internally and with the assistance of first responders. Building collaborative relationships with local law enforcement and responders (e.g., police, firefighters, and emergency medical services) prior to an incident helps ensure response personnel have an improved understanding of the facility's layout and hazards, maintain appropriate equipment and training to address facility hazards, and allow them to take quick and decisive action during an incident. Facilities should consider:

**The first time that local law enforcement or first responders actually access the facility should not be the day of an incident.**

- Including response personnel in the development and exercise of the response plan.
- Meeting regularly with first responders and sharing updates to emergency response plans.
- Creating a toolkit for responders that contains items like the facility emergency contacts, facility layout, safety data sheets, access credentials, and radio interoperability.
- Inviting local fire department and law enforcement for a tour of the facility.
- Participating in Local Emergency Planning Committee (LEPC) meetings.
- Conducting joint exercises with other organizations offsite.

## Tools and Resources

- RBPS 9 – Response: cisa.gov/rbps-9-response
- RBPS Guidance: cisa.gov/publication/cfats-rbps-guidance
- CFATS Resources: cisa.gov/cfats-resources
- CFATS information on the CISA Gateway: cisa.gov/cfats-eo13650 or ipgateway.dhs.gov/eo13650
- Request a Compliance Assistance Visit: cisa.gov/request-compliance-assistance-visit
- CFATS Knowledge Center: csat-help.dhs.gov
- Chemical Security Assessment Tool (CSAT) Help Desk (technical assistance): Call 1-866-323-2957 or email CSAT@hq.dhs.gov