IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CFATS Risk-Based Performance Standard (RBPS) 15-16 – Significant Security Incidents

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 15 – Reporting of Significant Security Incidents and RBPS 16 – Significant Security Incidents and Suspicious Activities at a Glance

The easiest way for a facility to prepare employees and security staff to do their part is to establish protocols clearly explaining what defines an incident as "significant" and written procedures on how to identify, respond to, and report the incident or activity to the appropriate facility personnel, local law enforcement, and/or CISA.

RBPS 15 and 16 complement each other and address the importance of having a process in place for promptly and adequately identifying, investigating, and reporting all significant security incidents and suspicious activities to appropriate entities.

Security Measures for Incidents

Facilities should consider establishing protocols for:

- Reporting an incident up the security chain of command of the facility and the company that owns or operates the facility.
- Defining what kinds of security incidents are "significant" and should be reported to CISA, other federal agencies (e.g., the FBI), and/or state or local law enforcement and first responders.

Facilities should also have written procedures, either in its security plan (Site Security Plan [SSP] or Alternative Security Program [ASP]) or elsewhere, to ensure that qualified personnel conduct thorough investigations of significant security incidents and suspicious activities to determine the level of threat, if vulnerabilities were exploited, and what security upgrades, if any, are warranted.

Significant Security Incidents (Physical and Cyber)

A broad number of events may be considered a security incident, including trespassing, vandalism, petty theft, cyberattacks, bomb threats, and armed attacks. It is generally within the facility's discretion to determine whether the incident is "significant" or not, and thus reported to CISA and local law enforcement.

Significant security incidents likely will include events that arise based on intentional threats that attempt to or successfully circumvent a security measure, including:

Avoiding cameras is a security incident.

- An intentional breach of the facility's restricted area or perimeter.
- An intentional act to forcefully or covertly bypass an access control point.
- Theft or diversion or suspected theft or diversion of a COI.
- An onsite fire, explosion, release of a COI, or other incident requiring the attention of local first responders.
- Any incident with malicious intent to adversely affect critical cyber assets, including information technology (IT) equipment.

Suspicious Activities

Suspicious activities could include a pattern of suspicious people or vehicles in or near the facility, photographing of the facility, or other unusual activity indicating that an adversary may be probing or assessing the facility's security capabilities. This may also include suspicious COI orders from unknown customers, customers who request cash payments, or delivery to unknown locations or businesses.

Reporting an Incident

If a significant security incident is detected while in progress, the facility should immediately call local law enforcement and emergency responders via 9-1-1. Similarly, if the event has concluded but an immediate response is still necessary, the facility should immediately call 9-1-1.

Once the incident has concluded and any resulting emergency has been addressed, the facility should use a nonemergency number to call local first responders and other federal, state, and local law enforcement entities, as applicable.

Reporting an Incident to CISA

Once an incident has concluded and any emergency has been addressed, report significant cyber and physical incidents to CISA Central at central@cisa.gov.

CISA Central provides a critical infrastructure 24/7 watch and warning function, and gives all critical infrastructure owners and operators a means to connect with and receive information from all CISA services. Learn more at cisa.gov/central.

Tools and Resources

- RBPS 15 and 16 – Significant Security Incidents: cisa.gov/rbps-1516-security-incidents
- RBPS Guidance: cisa.gov/publication/cfats-rbps-guidance
- CFATS Resources: cisa.gov/cfats-resources
- Request a Compliance Assistance Visit: cisa.gov/request-compliance-assistance-visit
- CISA Central: cisa.gov/central
- 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