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

CFATS Risk-Based Performance Standard (RBPS) 1-7 – Detection and Delay

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 Overarching Security Objectives

Generally, a facility's security measures that address appropriate RBPS will fall within one of five overarching security objectives:

1. Detection
2. Delay
3. Response
4. Cyber
5. Security Management

These are the overall security objectives that the individual RBPS address and may assist facilities to take a holistic approach to their security posture. Each objective spans multiple RBPS and can be satisfied through one or more of those RBPS.

RBPS 1-7 – Detection and Delay Overview

Detecting and delaying an intrusion or attack is a critical component of facility security. These two objectives address multiple RBPS:

- RBPS 1: Restrict Area Perimeter
- RBPS 2: Secure Site Assets
- RBPS 3: Screen and Control Access
- RBPS 4: Deter, Detect, and Delay
- RBPS 5: Shipping, Receipt, and Storage
- RBPS 6: Theft or Diversion
- RBPS 7: Sabotage

The specific capability and security measures required by each RBPS depend not only on the tier of the facility, but also on the security issue(s) related to the chemical(s) of interest (COI) at the facility. Thus, each facility and its specific posture—including the state of the COI, packaging, and existing mitigation measures—must be taken into account when determining what security measures to put into place.

Detection

For a protective system to prevail, detection needs to occur prior to an attack (i.e., in the attack-planning stages) or early enough in the attack where there is sufficient delay between the point of detection and the successful conclusion of the attack for the arrival of adequate response personnel. When evaluating detection measures, different types of attacks and outcomes should be taken into account. For example:

- A theft/diversion attack becomes successful when the COI is taken offsite through theft or deception and utilized in an attack. Theft facilities should detect the action prior to its success.
- A release attack becomes successful when the release affects the targeted population. Releases vary depending on whether they are toxic, flammable, or explosive. A toxic release is dependent on the release rate (can occur slowly) and can be mitigated by containments or other measures, whereas an explosive release happens instantly with little mitigation to slow or stop the effects.

- A successful sabotage attack occurs offsite as a result of onsite tampering, so detection of tampering at the point of shipment is most appropriate for these facilities.

When evaluating appropriate detection measures, a facility should take into account its tier and security issues. For example:[1]

<table>
<tr><th>Security Issue</th><th colspan="2">Tier 1</th><th>Tier 2</th><th>Tier 3</th><th>Tier 4</th></tr>
<tr><td>Theft/Diversion</td><td colspan="2" rowspan="3">Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion to a continuously manned location. This may be achieved by physical security systems (e.g., an intrusion detection system [IDS] or closed circuit television [CCTV]), personnel presence, or a combination thereof, with no gaps.</td><td>Maintain reasonable ability to detect and initiate a response in real time (for example, ensuring monitoring systems are checked multiple times a day, including weekends).</td><td>Maintain some ability to detect and initiate a response (for example, ensuring monitoring systems are checked at least once a day, including weekends).</td></tr>
<tr><td>Release</td><td colspan="2">Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion in real time. This may be achieved by physical security systems or personnel presence, or a combination thereof, with no gaps, OR via process alarms with automatic mitigation measures.[2]</td></tr>
<tr><td>Sabotage</td><td colspan="2">Maintain ability to detect attempted tampering prior to shipment. This may include traditional detection methods or perimeter-based detection of incoming substances through ingress screening and inspections or shipping procedures requiring inspection prior to egress.</td></tr>
</table>

Delay

A facility should be able to delay an attack for a sufficient period of time to allow appropriate response by security personnel via barriers and barricades (e.g., fencing, walls, locking mechanisms, bollards, etc.) and hardened targets. For example, Tier 1 and Tier 2 facilities should maintain multiple layers of delay, while Tier 3 and Tier 4 facilities should have some deterrence ability.

When evaluating delay measures, a facility should take into account its security issues. Release facilities should consider strong vehicle barriers and sufficient vehicle standoff distances around the COI. The required standoff distances vary depending on the building components used in the facility's construction.

<table>
<tr><th>Security Issue</th><th colspan="2">Tier 1</th><th>Tier 2</th><th>Tier 3</th><th>Tier 4</th></tr>
<tr><td>All security issues</td><td colspan="2">Facilities should maintain multiple layers of delay.</td><td colspan="2">Facilities may establish one level of delay in combination with appropriate detection measures.</td></tr>
</table>

Tools and Resources

- CFATS RBPS 1-7 Detection and Delay: cisa.gov/rbps-1-7-detection-delay
- 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
- 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

[1] All security measures in this fact sheet are possible, nonexclusive examples for facilities to consider as part of their overall strategy to address RBPS and are not prerequisites to CFATS compliance. A facility can propose other means to satisfy RBPS.

[2] Release-Toxic facilities with automatic mitigation measures—e.g., dikes or other containment measures—that would be successful in reducing the effects of the attack or slow the release from impacting the targeted population may not require continuous intrusion detection if they have a detection capability at the moment of the release through process alarm or similar device. Release-Flammable facilities with strong mitigation measures—e.g., automatic deluge system that suppresses fire through extinguishing materials such as water, foam, dry powder chemicals, or inert gases—that would be successful in preventing an attack may also not require continuous intrusion detection if they have a detection capability at the moment of the release such as a heat sensor or similar device.