



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

# CFATS Risk-Based Performance Standard (RBPS) 18 – Records



DEFEND TODAY,  
SECURE TOMORROW

## 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 18 – Records at a Glance

The development and maintenance of records may help facilities prepare for a response to a security incident, identify security gaps, ensure security equipment is in good working order, and verify facility personnel are familiar with security procedures.

**RBPS 18 – Records addresses the creation, maintenance, protection, storage, and disposal of specific security-related records pursuant to 6 CFR § 27.255. These records must be available to CISA upon request.**

## Record Types and Requirements

Under CFATS, all records required to be created or retained are Chemical-terrorism Vulnerability Information (CVI) (6 CFR § 27.400((b)(6))) and must be protected, maintained, and marked as such, unless records under items 1–5 were created to satisfy other regulatory requirements. Records must be retained for at least three years and include:

1. Trainings
2. Drills and exercises
3. Incidents and breaches of security
4. Maintenance, calibration, and testing of security equipment
5. Security threats
6. Audits of Site Security Plan (SSP) or Alternative Security Program (ASP)
7. Letters of Authorization and Approval

### Training Records

Under RBPS 11 – Training, the records for training must include:

- Date and location of each training session
- Time of day and duration of each session
- Description of the training
- Name(s) and qualifications of the instructor(s)
- List of attendees (including signatures)
- At least one unique identifier of each attendee receiving training
- Results of any evaluation or testing

### Records of Drills and Exercises

To satisfy RBPS 9 – Response and RBPS 11 – Training, records of drills and exercises that are part of the facility's training program to prepare its personnel to respond to incidents must include:

- Date held and description of drill/exercise
- List of participants
- List of equipment (excluding personal equipment) tested or employed
- Name(s) and qualifications of exercise director(s)
- Best practices or lessons learned that may improve the SSP

CISA | DEFEND TODAY, SECURE TOMORROW



[cisa.gov/cfats](https://cisa.gov/cfats)



[CFATS@hq.dhs.gov](mailto:CFATS@hq.dhs.gov)



[Linkedin.com/company/cisagov](https://www.linkedin.com/company/cisagov)



[@CISAgov](https://twitter.com/CISAgov) | [@cyber](https://twitter.com/cyber) | [@uscert\\_gov](https://twitter.com/uscert_gov)



[Facebook.com/CISA](https://www.facebook.com/CISA)



[@cisagov](https://www.instagram.com/cisagov)

## Records of Security Incidents

In conjunction with RBPS 15 – Reporting of Significant Security Incidents and RBPS 16 – Significant Security Incidents and Suspicious Activities, records of incidents and security breaches must include:

- Date and time of occurrence
- Location within the facility
- Description of the incident or breach
- Name(s) to whom it was reported
- Description of the response

## Maintenance Records

Under RBPS 10 – Monitoring, records of maintenance, calibration, and testing of security equipment must include:

- Date and time
- Name(s) and qualifications of the technician(s)
- Specific security equipment involved in maintenance, calibration, and testing

Records may be handled by third-party contractors but must be available to CISA upon request.

## Records of Security Threats

In conjunction with RBPS 13 – Elevated Threats and RBPS 14 – Specific Threats, Vulnerabilities, or Risks, records of security threats must include:

- Date and time of occurrence
- How the threat was communicated
- Name(s) of who received/identified the threat
- Description of the threat
- Name(s) to whom it was reported
- Description of the response

## Audit Records

Under RBPS 18 – Records, records of SSP/ASP audits must include:

- Date of the audit
- Results of the audit
- Name(s) of who conducted audit
- Letter (or similar document) certified by the facility with date the audit was conducted

The first audit must be completed 12 months after the SSP/ASP approval and annually thereafter.

## Voluntary RBPS 18 Sample Records

CISA has identified industry best practices in developing and maintaining these records, and used them to create voluntary sample records (e.g., sample record of security threats). The sample records may help facilities comply with RBPS 18 and can be tailored to the facility's specific needs. Download the RBPS 18 Sample Records at [cisa.gov/publication/cfats-rbps-18-records](https://cisa.gov/publication/cfats-rbps-18-records).

## Tools and Resources

- RBPS 18 – Records: [cisa.gov/rbps-18-records](https://cisa.gov/rbps-18-records)
- RBPS Guidance: [cisa.gov/publication/cfats-rbps-guidance](https://cisa.gov/publication/cfats-rbps-guidance)
- CFATS Resources: [cisa.gov/cfats-resources](https://cisa.gov/cfats-resources)
- CVI: [cisa.gov/chemical-terrorism-vulnerability-information](https://cisa.gov/chemical-terrorism-vulnerability-information)
- CFATS Knowledge Center: [csat-help.dhs.gov](https://csat-help.dhs.gov)
- Request a Compliance Assistance Visit: [cisa.gov/request-compliance-assistance-visit](https://cisa.gov/request-compliance-assistance-visit)
- Chemical Security Assessment Tool (CSAT) Help Desk (technical assistance):  
Call 1-866-323-2957 or email [CSAT@hq.dhs.gov](mailto:CSAT@hq.dhs.gov)