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

CFATS Risk-Based Performance Standard (RBPS) 8 – Cyber

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 8 – Cyber at a Glance

Cyber systems are integrated throughout the operations of chemical facilities, including controlling sensitive processes, granting authorized access, and enabling business. Even seemingly noncritical systems may provide backdoor access to systems that manage critical processes. Good cybersecurity posture means taking a comprehensive view of all cyber systems and using a layered approach of policies, practices, and people to prevent, protect against, respond to, and recover from cyber sabotage or incidents, such as a denial-of-service attack, virus, worm, botnet, and more.

RBPS 8 – Cyber is the performance standard to deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, business systems, and other sensitive computerized systems.

Critical Cyber Systems under CFATS

Systems that a facility may consider critical include, but are not limited to, those that:

1. Monitor or control physical processes that contain a COI.
2. Contain business or personal data that could be exploited to steal, divert, or sabotage a COI.
3. Connect to other cyber physical systems (CPS) that manage physical processes that contain or affect the security of a COI.
4. Are identified as information technology (IT), operational technology (OT), or communications systems.
5. Connect to the Internet of Things (IoT).

In the cybersecurity section of a facility's security plan—Site Security Plan (SSP) or Alternative Security Program (ASP)—the facility should list all its cyber systems and describe how the measures will protect these systems from attacks that could cause a COI to be released, diverted, or stolen. The level of cyber protections expected at a facility increases in correlation to the level of cyber integration.

Note: Security measures should apply regardless of the cyber system's location (e.g., on site, corporate headquarters, or vendor's location).

Critical Business Systems

Facilities with critical systems that contain business or personal data (e.g., inventory management system) should consider measures to:

- Develop, maintain, and implement documented and distributed cybersecurity policies and procedures, including change management policies, as applicable, to critical cyber assets.
- Maintain account access control utilizing the least privilege concept, maintain access control lists, and ensure that accounts with access to critical/sensitive data or processes are modified, deleted, or deactivated immediately when the user leaves or no longer requires access.

- Implement password management protocols to enforce password structures, change all default passwords (where possible), and implement physical controls for cyber systems where changing default passwords is not technically feasible.
- Restrict physical access to cyber assets and media to authorized users and affected individuals.
- Report significant cyber incidents to senior management and CISA Central at central@cisa.gov (cisa.gov/central).
- Train employees and contractors who work with cyber assets, as appropriate, in cybersecurity.

Critial Physical Security Systems

Facilities that use remote connections to access physical security systems connected to the security of COI should consider measures to:

- Define allowable remote access (e.g., internet, virtual private network [VPN], gateways, routers, modems, firewalls, wireless access points, vendor maintenance connections, Internet Protocol [IP], and address ranges), user responsibilities, and rules of behavior for remote access issues.

Critical Control Systems

Facilities with critical systems (e.g., Supervisory Control and Data Acquisition [SCADA] systems, Distributed Control Systems [DCSs], Process Control Systems [PCSs], and Industrial Control Systems [ICSs]) that monitor and/or control physical processes containing a COI should consider measures to:

- Conduct recurring audits that measure compliance with the cybersecurity policies, plans, and procedures, and report results to senior management.
- Document the business need and network/system architecture for all critical cyber systems.
- Disable unnecessary system elements upon identification, identify and evaluate potential vulnerabilities, and implement appropriate compensatory security controls.
- Identify and document systems boundaries, and implement security controls to limit access across those boundaries.
- Maintain a defined incident response system for possible cyber incidents.
- Integrate cybersecurity into the system lifecycle for all critical cyber assets from system design through procurement, implementation, operation, and disposal.
- Monitor the critical networks in real time for unauthorized or malicious access and alerts, and recognize and log events and incidents.
- Integrate backup power for all critical cyber systems should an emergency or incident occur.
- Maintain continuity of operations plans, IT contingency plans, and/or disaster recovery plans.

Tools and Resources

- RBPS 8 – Cyber: cisa.gov/rbps-8-cyber
- RBPS Guidance: cisa.gov/publication/cfats-rbps-guidance
- CFATS Resources: cisa.gov/cfats-resources
- CISA's Cyber Resource Hub: cisa.gov/cyber-resource-hub
- Computer Security Resource Center: csrc.nist.gov
- Security and Privacy Controls for Federal Information Systems and Organizations: csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- Chemical Sector Cybersecurity Framework Implementation Guidance: cisa.gov/publication/chemical-cybersecurity-framework-implementation-guidance
- Request a Compliance Assistance Visit: 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