



The Chemical Facility Anti-Terrorism Standards (CFATS) program, identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with regulated chemicals. Under CFATS, facilities that DHS has determined to be high-risk are required to develop and implement security plans that meet applicable risk-based performance standards (RBPS).

### The Importance of Cybersecurity CFATS Facilities

Protecting against cyber sabotage, such as cyber intrusions, worm attacks, and viruses, is an essential component in managing overall risk for a facility. The goal of cybersecurity is to reduce the risk of attackers conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage of chemicals of interest (COI). A comprehensive approach of appropriate security policies, practices, and people to prevent, protect, respond to, and recover from incidents helps deter cyber sabotage.

### How DHS Evaluates Cybersecurity Measures under CFATS

Cybersecurity typically involves policies and procedures that protect a facility's critical systems. Systems that a facility may consider critical include, but are not limited to, those that:

- (1) Contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI;
- (2) Are connected to other systems that manage physical processes that contain a COI; or
- (3) Monitor and/or control physical processes that contain a COI.

Specific examples of cyber systems that a facility may wish to consider critical are identified in the RBPS Guidance Document.

When reviewing the cybersecurity section of either a Site Security Plan (SSP) or Alternative Security Program (ASP), DHS considers the type of cyber assets, including control and business systems, and what enhanced security measures would be appropriate to the different types of systems. The level and degree of cyber protections expected at facilities increases in correlation to the level of cyber integration. When thinking about cybersecurity as it relates to CFATS, facilities should keep in mind their COI(s) and the specific security issue. The cybersecurity measures described should address how cybersecurity systems impact the security of the COI and how they are used to protect the critical cyber systems from attacks that could cause a release or divert or steal the COI, depending on the respective security issues(s). To better assist facilities in addressing RBPS 8, the following summarizes security measures for consideration based on a facility's system, as outlined in the Expedited Approval Program and RBPS Guidance documents.

#### Critical Business Systems

Facilities with critical business systems, such as an inventory management system, that fall into the first category—business systems that, if exploited, could result in the theft, diversion, or sabotage of a COI—should consider several security measures:

- Develop, maintain, and implement documented and distributed cybersecurity policies and procedures including change management policies, as applicable, to their critical cyber assets. Appropriate cybersecurity policies should cover all aspects of cybersecurity measures, as applicable to the facility.
- Maintain account access control to critical cyber systems utilizing the least privilege concept, maintain access control lists, and ensure that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated immediately when personnel leave and/or when users no longer require access.

#### RBPS 8 - Cyber

Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs), critical business systems, and other sensitive computerized systems.

- Implement password management protocols to enforce password structures, ensure all default passwords have been changed (where possible), and implement physical controls for cyber systems where changing default passwords is not technically feasible.
- Ensure that physical access to critical cyber assets and media is restricted to authorized users and affected individuals.
- Report significant cyber incidents to senior management and DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (<https://ics-cert.uscert.gov/>).
- Provide cybersecurity training for employees and contractors, as appropriate, who work with cyber assets.

### Critical Physical Security Systems

Often facilities that have physical security systems utilize these systems through remote connections. Therefore, facilities with remote access to systems that manage physical processes containing a COI should also consider this security measure:

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

### Critical Control Systems

Facilities with critical systems that monitor and/or control physical processes containing a COI should also consider a number of security measures:

- 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 assets.
- Disable unnecessary system elements upon their identification and 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 (i.e., denial-of-service attack, virus, worm attack, botnet, etc.).
- 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 incidents occur.
- Maintain continuity of operations plans, IT contingency plans, and/or disaster recovery plans.

### Additional References and Resources

- Risk-Based Performance Standards Guidance Document: <https://www.dhs.gov/publication/cfats-rbps-guidance>
- DHS Guidance for the Expedited Approval Program: <https://www.dhs.gov/cfats-expedited-approval-program>
- Computer Security Resource Center: <http://csrc.nist.gov/>
- Generally Accepted Principles and Practices for Securing Information Technology Systems: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>
- Security and Privacy Controls for Federal Information Systems and Organizations: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- Chemical Sector Cybersecurity Framework Implementation Guidance: <https://www.dhs.gov/publication/chemical-cybersecurity-framework-implementation-guidance>

