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

Chemical Facility Anti-Terrorism Standards: Reporting Cyber Incidents

Overview

The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) program 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.

This resource provides an overview of RBPS 8 – Cyber and RBPS 15 – Reporting of Significant Security Incidents, which require facilities covered under the CFATS program to establish protocols for identifying and reporting significant cyber incidents to appropriate facility personnel, local law enforcement, and CISA.

Examples of Critical Cyber Systems

Cyber systems may be integrated throughout the operations of chemical facilities, including controlling sensitive processes, granting authorized access, and enabling business. Systems that a facility may consider critical are systems related to controlling, processing, or accessing COI, which may include, but are not limited to:

- A control system (including a remotely operated control system) that directly monitors and/or controls manufacturing or other physical processes that contain COI.
- A business system at the headquarters office that manages ordering and/or shipping of a COI.
- A business system (at the facility, headquarters office, or third party) that contains personally identifiable information for those individuals (e.g., facility personnel, customers) who could be exploited to steal, divert, or sabotage a COI.
- An access control or security monitoring system that is connected to other systems.
- Enterprise resource planning systems that conduct critical functions in support of chemical processes for COI or a COI supply chain activity.
- Email and fax systems used to transmit sensitive information related to ordering and/or shipping of a COI.
- A noncritical control system on the same network as a critical control system.
- A sales system that is connected to the data historian for a critical control system.
- A watchdog system or Safety Instrumented System (SIS) for a critical control system.
- A system hosting critical or sensitive information that, if exploited, could result in the theft or diversion of a COI or sabotage its processing (e.g., website, intranet).

A cyberattack can have significant physical consequences—especially in a high-risk chemical facility that possesses systems vulnerable to cyber sabotage. Even seemingly noncritical systems may provide backdoor access to systems that manage critical processes. Having a 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 incidents.

Examples of Cyber Incidents

Incidents that could be assessed as significant cyber incidents that high-risk facilities should consider reporting to CISA include, but are not limited to:

- Known security issues, vulnerabilities, and exploits that impact the COI asset areas or system.
- Attempts to gain unauthorized access to a critical cyber system.
- Threats to operational technology (OT) (e.g., Supervisory Control and Data Acquisition [SCADA] systems, Distributed Control Systems [DCSs], Process Control Systems [PCSs], Industrial Control Systems [ICSs]).
- Ransomware incidents.

- Phishing, malware, trojan horse, or virus attacks that were not contained using cybersecurity software tools, practices, and techniques.
- Structured Query Language (SQL) injections where malicious code is injected into a server and forces it to disclose private data.
- Attempts to gain unauthorized access to a system's wireless network or mobile devices on the network.
- Changes to a system's firmware, software, or hardware without the system owners' consent.
- Disruption or denial of service (DOS), or distributed denial of service (DDOS) attempts.
- Any effects on critical infrastructure or core government functions; or impacts to national security, economic security, or public health and safety systems.

Before an Incident

The easiest way for a facility to prepare its employees to do their part is to clearly explain to them—and especially to its security staff—how to identify, respond to, and report a cyber incident. In the cybersecurity section of a facility's Site Security Plan (SSP) or Alternative Security Program (ASP), the facility should list all its cyber systems, describe how the measures will protect these systems, and provide reporting protocols for a cyber incident. Before a cyber incident, the facility should identify to whom an incident will be reported.

Contacts To Report Significant Cyber Incidents

- **CISA Central: Central@cisa.gov**
- **Facility Cybersecurity Officer: _____**
- **Facility Security Officer: _____**
- **Chemical Security Inspector: _____**

Reporting a Cyber Incident to CISA

Information sharing is integral as warnings of attacks, incidents, and network abnormalities can reduce the number of victims and lessen the impact. Once a cyber incident has been detected and response measures in the facility's security plan have been initiated, high-risk facilities are required to report significant cyber incidents to CISA via CISA Central (central@cisa.gov) in accordance with their SSP or ASP.

When contacting CISA Central, facilities should indicate they are "critical infrastructure" and within the Chemical Sector. Facilities should also include a description of the incident, indicate that they are regulated under CFATS, and include the facility identification number (i.e., FID) issued to them by CISA when they registered their facility in the Chemical Security Assessment Tool (CSAT).

After an Incident

Facilities are expected to retain the incident reporting number issued to them as evidence that they have complied with the significant incident reporting requirements under RBPS 15. Generally, a Chemical Security Inspector follows up on the incident report and subsequently conducts an interview that may solicit additional information. Facilities should be prepared to provide the incident number to the Chemical Security Inspector.

Tools and Resources

- RBPS 8 – Cyber: cisa.gov/rbps-8-cyber
- RBPS 15 and 16 – Significant Security Incidents: cisa.gov/rbps-1516-security-incidents
- CFATS Resources: cisa.gov/cfats-resources
- CISA's Role in Industrial Control Systems: cisa.gov/ics
- CISA Cyber Resource Hub: cisa.gov/cyber-resource-hub
- Local Federal Bureau of Investigation (FBI) Offices: fbi.gov/contact-us/field-offices
- Chemical Sector Cybersecurity Framework Implementation Guidance: cisa.gov/publication/chemical-cybersecurity-framework-implementation-guidance
- Computer Security Resource Center: csrc.nist.gov