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

Chemical Facility Anti-Terrorism Standards (CFATS) and the CISA Gateway

Overview

The Cybersecurity and Infrastructure Security Agency (CISA) Gateway serves as the single interface through which federal, state, local, tribal, territorial, and private sector partners can identify, analyze, and manage risk. Some Chemical Facility Anti-Terrorism Standards (CFATS) program information—such as facilities with hazardous chemicals that could be weaponized—can be accessed via the CISA Gateway for entities with a need to know to enhance emergency response and preparedness.

Coordination and Information Sharing

Executive Order (EO) 13650: Improving Chemical Facility Safety and Security was signed to improve the safety and security of chemical facilities and reduce the risks of hazardous chemicals to workers and communities. The EO directed federal agencies to improve coordination and information sharing with state and local governments, and community stakeholders to ensure they have access to key information to prevent, prepare for, and respond to chemical incidents.

In response, the Department of Homeland Security (DHS), Department of Labor, Environmental Protection Agency, Department of Justice, Department of Agriculture, and Department of Transportation, as part of an interagency working group, worked to establish priority actions; modernize policies, regulations, and standards; and implement findings based on lessons learned and feedback from industry.

What Is CFATS?

In 2006, Congress authorized DHS to establish the Chemical Facility Anti-Terrorism Standards (CFATS) program. Managed by CISA, the CFATS program identifies and regulates high-risk chemical facilities to ensure security measures are in place to reduce the risk of certain hazardous chemicals being weaponized. Appendix A of the CFATS regulation (6 CFR Part 27) lists more than 300 chemicals of interest (COI) and the respective screening threshold quantities (STQ) that are categorized into three main security issues: release, theft or diversion, and sabotage. Facilities that possess COI at or above STQ must complete a Top-Screen survey to report those chemicals. CISA reviews this information to determine which facilities are high-risk and assigns them a tier. Tiered facilities are required to implement security measures that reduce the risks associated with the COI.

What Is the CISA Gateway?

Information systems play a vital role in allowing federal departments; state, local, tribal, and territorial (SLTT) governments; and private sector partners identify, analyze, and manage risk to protect the nation. CISA established the CISA Gateway to improve information sharing and coordination among federal and SLTT agencies. This centrally managed repository of data and capabilities allows stakeholders to easily access, search, retrieve, visualize, analyze, and export infrastructure data from multiple sources. The CISA Gateway maintains three layers of information protection:

- Protected Critical Infrastructure Information (PCII)
- Chemical-terrorism Vulnerability Information (CVI)
- For Official Use Only (FOUO)

These protections are role-based (or permission-based), giving CISA stakeholders confidence that sharing information with the federal government and other stakeholders will not expose sensitive or proprietary data.

What CFATS Information Is Available on the CISA Gateway?

Through the CISA Gateway, CISA shares certain CFATS data elements on a geospatial map to help communities identify and prioritize risks and develop a contingency plan to address those risks. CFATS data is available in a FOUO layer and a CVI layer to authorized federal agencies, SLTT officials, and first responders with an established need to know as determined by CISA.

Via the CISA Gateway, information on chemical facilities is available to federal and SLTT officials with an established need to know.

FOUO access allows users to view information on a chemical facility (such as name, location, and geospatial information) within their state, county, and surrounding counties, whereas CVI access includes additional information, such as CFATS tiers. This permission-based system allows CISA to share CFATS information while appropriately balancing security risks and ensuring regulators will not have access to existing PCII data.

Who Can Access CFATS Information on the CISA Gateway?

Personnel who want to view CFATS information on the CISA Gateway must be PCII certified, complete required CISA Gateway training, complete CVI training, and have a valid need to know. Personnel with direct regulatory responsibilities who want to view CFATS data on the CISA Gateway are only authorized to access the data via the CISA Gateway EO 13650 Portal. Personnel without direct regulatory responsibilities may obtain access to the information via the CISA Gateway or the EO 13650 Portal.

- For PCII Training, please visit cisa.gov/pcii-authorized-user-training.
- For CVI Training, please visit cisa.gov/cvi-authorized-user-training.

How Do I Gain Access to the CISA Gateway?

After completing PCII and CVI authorized user training, visit eo13650.gateway.cisa.gov, click the "Request an IP Gateway EO 13650 account here" link, and fill out the online form. Email CISA-GatewayHelpdesk@cisa.dhs.gov with any questions or concerns accessing the CISA Gateway.

Tools and Resources

- Request a CFATS Presentation: cisa.gov/request-cfats-presentation
- CFATS and Executive Order (EO) 13650: cisa.gov/cfats-eo13650
- CISA Gateway: cisa.gov/cisa-gateway or eo13650.gateway.cisa.gov
- PCII Program: cisa.gov/pcii-program
- CFATS Program: cisa.gov/cfats
- CVI: cisa.gov/chemical-terrorism-vulnerability-information
- CFATS Knowledge Center: csat-help.dhs.gov