CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)

What To Expect When You're Inspected?

Craig Conway, December 8th, 2020

Discussion Objectives

Demystifying the Inspection Process

- Provide insight into the inspection process
- Reduce new facility anxiety
- Provide helpful guidance
- Share our organization's COVID-19 adaptations

Discussion Outline

CFATS Inspection Discussion

- Brief background
  - Who are we?
  - What do we inspect?
- How are facilities evaluated?
- How to “Ace” an inspection?
- How has the pandemic changed inspections?

What is CFATS?

Chemical Facility Anti-Terrorism Standards

The CFATS program identifies and regulates high-risk chemical facilities to ensure they implement appropriate security measures to reduce the risk of a terrorist attack associated with more than 300 chemicals of interest (COI). Facilities that store, manufacture, or distribute COI at screening threshold quantities and concentrations must report their holdings to DHS and comply with the CFATS standards.

- CFATS follows a risk-based approach, allowing DHS to focus on high-risk chemical facilities in accordance with their specific level of risk

What does CFATS mean by:

Risk-Based Decisions

Generally: Risk is an evaluation of potential consequence calculations adjusted by likelihood.

DHS Specific: Risk = Threat x Vulnerability x Consequence

Typically Threat and Vulnerability are fractions.

What Is Risk-Based Tiering?

The CFATS regulation follows a risk-based approach that allows CISA to focus its resources on high-risk chemical facilities. To identify a facility's specific level of risk, CISA analyzes information submitted through the Top-Screen to determine which facilities are high-risk and assigns those facilities to one of four tiers, with Tier 1 representing the highest risk.

What kinds of Threats does DHS evaluate?

Security Issue	Hazard	Attack Scenarios
Onsite Release	Release Toxics	Assault Team
	Release Flammables	Vehicle Explosive
	Release Explosives	
Theft/Diversion	Weapons of Mass Effect	Off-site Consequence
	Chemical Weapon Precursors	
	Explosive Precursors	
Sabotage/Contamination	Inhalation Toxic Precursors	Road/Rail Shipments

Which Agency Manages CFATS?

Cybersecurity and Infrastructure Security Agency (CISA)

In 2018, Congress created CISA from the former National Protection and Programs Directorate.

The Chemical Security Program Office falls under the Infrastructure Security Divison of CISA.

Chemical Security Inspectors (CSIs) are a specialized sub-group of security advisors with specific training to evaluate chemical specific risk scenarios.

Who are your local CSIs?

- Colorado is part of Region VIII which includes:
  - **7 Chemical Security Inspectors**
  - **1 Chief of Chemical Security**
  - **1 Regulatory Analyst**
- Inspectors visit regulated facilities to ensure that they meet the security requirements set by the CFATS program.

Tier	Facilities Currently Covered in the US	Facilities Currently Covered in Colorado
1	171	0
2	81	1
3	1,395	20
4	1,632	11
Total	**3,279**	**32**

Who does CFATS regulate?

CFATS facilities span across numerous industries

Chemical Facilities Come in All Shapes and Sizes

Chemical Manufacturing	Oil Refineries	Food Processing	Wineries	Colleges and Universities	Farm Cooperatives

- Schools & Universities
- Breweries
- Meat Packing facilities
- Agricultural supply & Processing facilities
- Prisons
- National Parks
- Mining
- Petrochemical
- Chemical Distributors
- Racetracks
- Water parks & Pools
- Laboratories
- Hospitals

What Requirements do Inspections Verify?

- Risk-Based Performance Standards (RBPS) are the foundation of a facility's Site Security Plan and drive the security standards at all tiered facilities.
- RBPS provide facilities with flexibility and allow for the use of existing or planned measures, ideas, and expertise where appropriate.
- A covered high-risk facility has to satisfy the applicable RBPS by implementing security measures appropriate to the facility's risk tier.
- Security measures appropriate to satisfy the RBPS will vary from one facility to another based upon level of risk and unique facility circumstances.

Risk-Based Performance Standards

1) Restrict Area Perimeter

2) Secure Site Assets

3) Screen and Control Access

4) Deter, Detect, Delay

5) Shipping, Receipt, and Storage

6) Theft and Diversion

7) Sabotage

8) Cyber

9) Response

10) Monitoring

11) Training

12) Personnel Surety

13) Elevated Threats

14) Specific Threats, Vulnerabilities, or Risks

15) Reporting Significant Security Incidents

16) Significant Security Incidents and Suspicious Activities

17) Officials and Organization

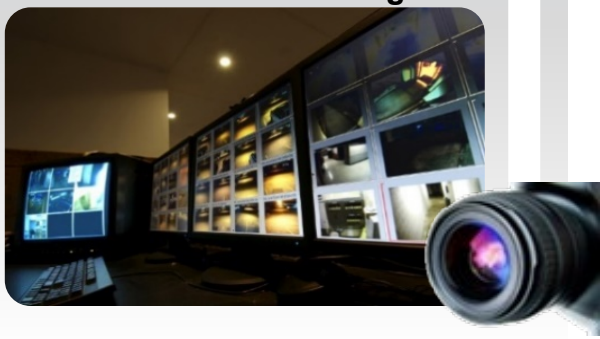
18) Records

- Compliance with the RBPS will be tailored to fit each facility's circumstances, including tier level, security issues, and physical and operating environments
- Rather than prescribe specific facility security measures, DHS developed 18 Risk-Based Performance Standards (RBPS)

RBPS-1 Restrict Area Perimeter

RBPS-8 Cyber

RBPS-10 Monitoring



Questions: Craig.Conway@hq.dhs.gov

Help tip:

Reminder, CFATS requirements are chemical and critical asset focused. They do not always extend to the whole property.

CFATS refers to this as an asset-based approach.

Overarching Security Objectives

DHS has grouped these 18 RBPS into 5 Security Objectives:

Detection

- Covers portions of Risk-Based Performance Standard (RBPS) 1-7

Delay

- Covers portions of RBPS 1-7

Response

- Covers portions of RBPS 11 and RBPS 9, 13-14

Cybersecurity

- Covers RBPS 8

Security Management

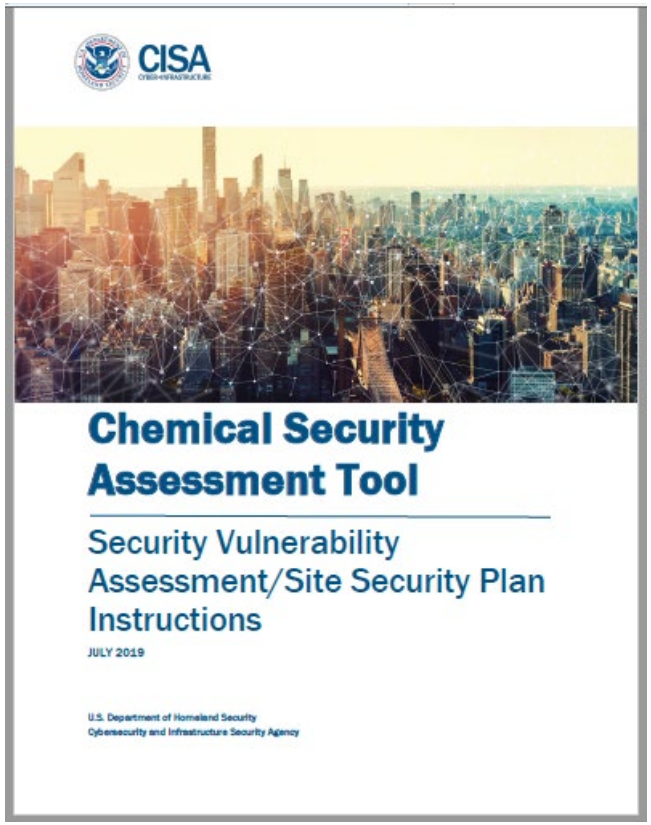
- Covers portions of RBPS 7 and 11 and RBPS 10, 12, and 15-18

Site Security Plan (SSP)

Updated in 2017

The SSP is how CFATS process fixes a flexible process into a verifiable plan appropriate for each individual facility.

Facilities propose their own solutions to functional requirements and CISA evaluates and approves plans in alignment with national standards.

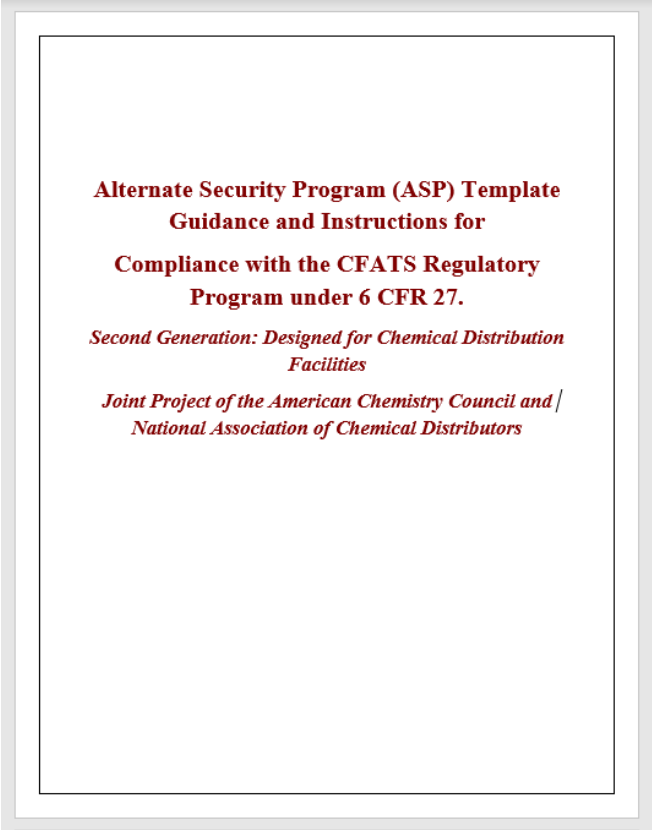


Alternative Security Plans

Additional flexibility to reduce regulatory burden

Any CFATS facility with a sufficient Security Plan of their own can choose to upload their existing plan instead of the standard CFATS template.

Several industries have worked together thru associations to pre-approve templates that work best for their industry segment.



Alternate Security Program (ASP) Template Guidance and Instructions for

Compliance with the CFATS Regulatory Program under 6 CFR 27.

Second Generation: Designed for Chemical Distribution Facilities

Joint Project of the American Chemistry Council and National Association of Chemical Distributors

Overarching Security Objectives

DHS has grouped these 18 RBPS into 5 Security Objectives:

Detection

- Covers portions of Risk-Based Performance Standard (RBPS) 1-7

Delay

- Covers portions of RBPS 1-7

Response

- Covers portions of RBPS 11 and RBPS 9, 13-14

Cybersecurity

- Covers RBPS 8

Security Management

- Covers portions of RBPS 7 and 11 and RBPS 10, 12, and 15-18

Detection

- If a facility chooses to utilize systems (IDS, ACS, or CCTV) for detection, DHS seeks to ensure they:
  - Cover the appropriate areas and/or entry points.
  - Are activated at appropriate times.
  - Alarm to a responsible and trained individual(s) in order to initiate a response.
- If the facility utilizes employees or on-site security personnel, they must:
  - Be capable and trained to provide detection.
  - Be dedicated to or conduct patrols of the necessary areas.

Delay

- A facility should be able to delay an attack for a sufficient period of time to allow appropriate response by security personnel via barriers and barricades—such as fencing, walls, locking mechanisms, bollards, etc.—and hardened targets.
- Delay measures should also take into account security issues, for example, a Release facility should also consider strong vehicle barriers and sufficient vehicle standoff distances around the COI. The required standoff distances will vary depending on the building components used in the construction of the facility.

Helpful tip:

CISA utilizes a “Holistic” based approach for detect and delay. As complimentary techniques, DHS recognizes that a facility with exceptional detection measures may require less delay measures, and vice versa.

Facilities with unique challenges or advantages can benefit from a holistic approach in order to more efficiently meet the standard.

CFATS Cyber Security

- Addresses the deterrence of cyber sabotage and unauthorized on-site or remote access to critical process controls, critical business systems, and other sensitive computerized systems.

The facility should develop a comprehensive approach to secure cyber systems and implement preventive measures to identify and address cyber vulnerabilities

RBPS 8 and Critical Cyber Systems

- When considering what systems could impact the security of the COI, facilities should examine:

Physical Security Systems

- An access control or security system that is connected to other systems
  - Does the facility employ an intrusion detection system or cameras?

Inventory Management

- A business system that manages the ordering / shipping of a COI
  - Does the facility utilize software to manage ordering, shipping, or inventory?

COI Processing

- A control system that monitors or controls physical processes that contain COI
  - Does the facility employ control systems (ICS, DCS, SCADA)?

Other systems to consider include:

- An access control or security system that is connected to other systems
- E-mail or fax systems used to transmit sensitive information related to COI
- A non-critical control system on the same network as a critical control system

Response

Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.

- Response focuses on the planning to mitigate, respond, and report incidents in a timely manner between facility personnel, first responders, and law enforcement
- Local Emergency Planning Committees (LEPC) may be contacted by local Chemical Security Inspectors to verify that facilities have developed plans for emergency notification, response, evacuation, etc.
- IP Gateway (EO Portal) – A DHS platform to share and coordinate CFATS information among Federal, State, local, territorial, and tribal (SLTT) agencies partners.

Security Management

Security Management is the capability to manage the SSP/ASP, including the development and implementation of policies, procedures and other processes that support Site Security Plan implementation and oversight.

Optional Assistance Anytime

No cost assistance with SSP development

The SSP is designed to be flexible. Not topic may be required at a given facility.

Facilities can often save time and cost by asking inspectors for options prior to assuming they need more security equipment.

For assistance, reach out to CFATS@HQ.dhs.gov or a local Inspector

Quick Recap

So far we've reviewed:

- What is the CFATS regulation?
- Who ensures compliance?
- What are the requirements?

But when should you actually expect an inspection?

When do Inspections Occur?

If the facility receives a tier…

- DHS provides compliance assistance upon request at any stage of this process

Inspection Frequency

Depends on type of Inspection

Authorization Inspections - Serve as the initial onsite inspection. As the first visit, these can typically take 1-2 full days.

Compliance Inspections - Re-occuring annual or biannual inspections that follow an Authorization inspection. Typically 2-8 hours depending on the facility.

What is an Authorization Inspection?

- Authorization Inspections are conducted at covered facilities to verify the facility content listed in the Site Security Plan (SSP) or Alternative Security Program (ASP) is accurate and that existing and planned measures satisfy the risk-based performance standards (RBPS).
- **DHS sends the facility a Letter of Authorization through CSAT**
- **A Chemical Security Inspector will reach out to the facility to discuss:**
  - A date and time for the inspection
  - The scope of the visit
  - The facility personnel required to be present
  - Required documents to be made available
  - Chemical-terrorism Vulnerability Information (CVI) considerations
  - Protective equipment and safety requirements

What is a Compliance Inspection?

- A Compliance Inspection (CI) is conducted as part of the recurring inspection process after a Letter of Approval has been issued to ensure the facility continues to implement its approved security plan

- **Compliance Inspections are conducted:**
  - To ensure that both existing and planned security measures that are identified in the approved SSP or ASP continue to be implemented fully and on schedule
  - To ensure that the equipment, processes, and procedures described in the SSP or ASP are appropriate and sufficient to meet the established risk-based performance standards
  - To ensure that required corrective actions have been implemented and are sustainable
  - To discuss other issues that have come up since the Letter of Approval

Inspection Process

Prior to Inspection:

1. Initial notification thru secure CSAT portal
2. Inspector coordination and logistics call
3. Inspector reviews all prior inspection reports
4. Optional: Remote document review session

Day of Inspection:

1. Arrival, presentation of credentials, and introductions
2. Site Safety Briefings
3. Site walk-thru of Chemical and Critical Assets locations
4. Testing of security equipment as applicable
5. Onsite seated interview and document review session
6. Optional onsite assistance with top-screen or SSP updates as needed

How to “Ace” a CFATS inspection

Facility and inspector best practices

All CFATS facilities are required to complete an annual audit of their own security program. DHS provides an example check-list style template. The audit is an excellent opportunity to identify any issues prior to the inspection.

After each inspection, an effective practice is to gather and staple all the documents reviewed into a secure CFATS folder for reference in future inspections.

Inspection Best Practices (continued)

Ask your inspector prior to the inspection what documents you can gather ahead of time. Time spent looking for documents is the main cause of longer inspection times.

Facility participation in a local emergency planning committees (LEPC) is an effective way to satisfy multiple CFATS Response standards.

Reach out to your inspector anytime to ask for help with security training requirements, drills or exercises.

What Penalties Exist for Non-Compliance?

- DHS's focus is on security, and the Department has a strong preference for working with facilities to help bring them into compliance
- DHS has the authority to fine a facility if it does not meet its regulatory obligations
  - For example, a facility that does not register for the CFATS program and is found to possess COI above STQ may be subject to fines.
- DHS has the authority to fine facilities up to $34,871 per day for each day the violation continues
- DHS reserves the right to issue an Order to Cease Operations for a facility's continuous failure to comply or for other serious violations

How have inspections changed during the Pandemic?

Risk Based Approach

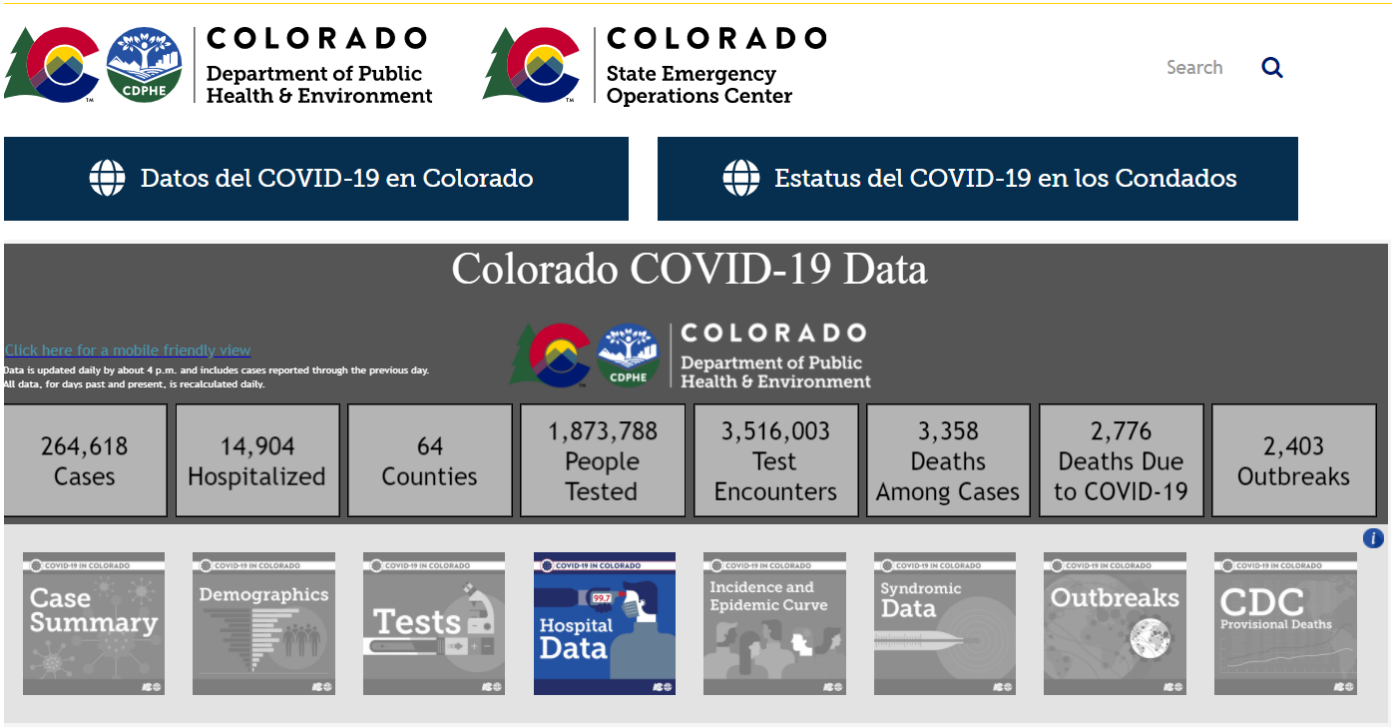
CISA follows all local, state and federal health guidelines to ensure public health.

Standard	Optional Hardship Extension Request System
Level 1	Adherence to Public Health Guidelines
Level 2	Distanced Outdoor Inspections
Level 3	Virtual Check-Ins

In addition CISA continues to evaluate and deploy risk based inspection protocols in coordination with industry stakeholders

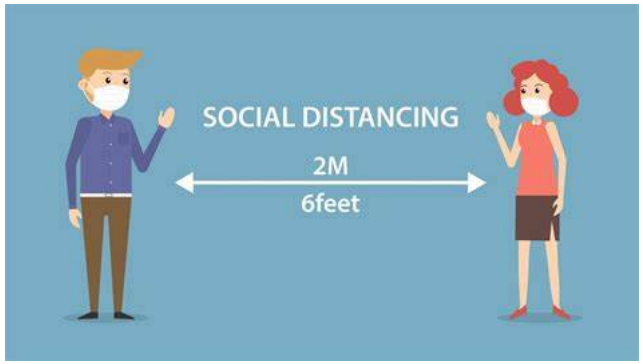
Risk-Based Inspection Scheduling

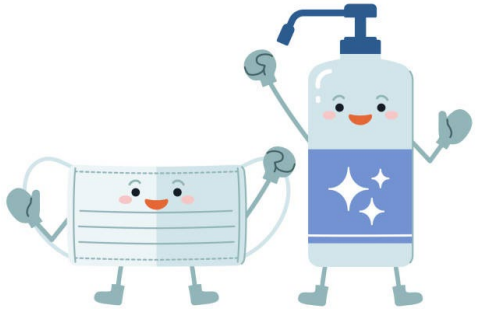
Review of County Level Data for Inspections



Questions: Craig.Conway@hq.dhs.gov

Base-Level Inspection Precautions





Inspector Travel Restrictions

Questions: Craig.Conway@hq.dhs.gov

Level 2: Outdoor Only Inspections

Risk based options allow flexible continuity

CFATS inspectors can situationally utilize remote meeting software to accomplish document review and interview portions of the inspection.

When appropriate, outdoor only inspections may still be utilized to verify chemical and physical security assets.

Questions: Craig.Conway@hq.dhs.gov

Level 3: Virtual Compliance Check-ins

Ensure continuing communication

Pilot program for COVID era challenges.

Maintains ability to review and discuss majority of RBPS metrics.

Reinforces critical elements of the incident reporting system – interpersonal relationships.

Review of Pandemic Mitigation Strategies

Risk Based Approach

CISA follows all local, state and federal health guidelines to ensure public health.

Standard	Optional Hardship Extension Request System
Level 1	Adherence to Public Health Guidelines
Level 2	Distanced Outdoor Inspections
Level 3	Virtual Check-Ins

In addition CISA continues to evaluate and deploy risk based inspection protocols in coordination with industry stakeholders

Navigating CISA.gov

1

CISA

REPORT

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

STRATEGIC INTENT

"DEFEND TODAY, SECURE TOMORROW"

ELECTION SECURITY | HOMETOWN SECURITY | CYBER ALERTS | CHINA MALICIOUS CYBER ACTIVITY | BE CYBER SMART | FEDERAL NETWORK SECURITY

2

CISA

REPORT

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

INFRASTRUCTURE SECURITY

CISA works with businesses, communities, and government at every level to help make the nation's critical infrastructure more resilient to cyber and physical threats. Everyone has a role securing the Nation's critical infrastructure.

Quick Links

2015 Sector Specific Plans
Chemical Security
Bombing Prevention
Critical Infrastructure Sector Partnerships
Critical Infrastructure Training
Critical Infrastructure Vulnerability Assessments
IDR Program
Hometown Security
Information Sharing: A Vital Resource
Insider Threat Mitigation
International Critical Infrastructure Engagement
Supporting Policy and Directive

CISA's Role in Infrastructure Security

Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The Nation's critical infrastructure provides the essential services that underpin American society.

CHEMICAL SECURITY | HOMETOWN SECURITY | ACTIVE SHOOTER PREPAREDNESS | RISK ASSESSMENTS | SCHOOL SAFETY & SECURITY

3

CISA

REPORT

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

Infrastructure Security > Chemical Security

Infrastructure Security

2015 Sector Specific Plans
Chemical Security
Critical Infrastructure Sector Partnerships
Critical Infrastructure Training
Critical Infrastructure Vulnerability Assessments
Dams Sector Resources
IDR Program
Information Sharing: A Vital Resource
Insider Threat Mitigation
International Critical Infrastructure Engagement
Hometown Security
Securing Soft Targets and Crowded Places

CHEMICAL SECURITY

Securing our Nation's chemical sector infrastructure is crucial to our economic prosperity, national security, and public health and safety.

Several thousand U.S. chemical facilities—from small companies to national laboratories—use, manufacture, store, transport, or deliver chemicals in a complex, global chain that affect other critical infrastructure sectors. From computer chips for biotechnology devices to the development of synthetic fibers that make firefighters clothes water and heat resistant, chemicals are used in the products and processes that impact our daily lives.

DHS has developed voluntary and regulatory programs and resources to help stakeholders—private industry, public sector, and law e[illegible]ment—secure chemical facilities from many threats: cyber attacks, biohazards, insider threats, and thef[illegible] diversion for use in chemical or explosive weapons. Enhancing security and resilience across the [illegible]ector requires a collaborative effort.

Chemical Facility Anti-Terrorism Standards
CFATS is a DHS regulatory program focused on security at high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with certain hazardous chemicals.

Ammonium Nitrate Security Program
The ANSP is a proposed regulatory program that seeks to reduce the likelihood of a terrorist attack involving the misuse of ammonium nitrate by creating a registration program for purchasers and sellers.

Chemical Sector Security Events
CISA sponsors events throughout the year to engage with stakeholders, exchange security-related information, and share best practices about chemical security.

Chemical Sector Resources
The Chemical Sector-Specific Agency provides institutional knowledge and specialized expertise to collaboratively develop, coordinate, and implement voluntary programs to improve security and resilience within the Chemical Sector.

Last Updated Date: September 10, 2019

4

CISA

REPORT

CYBERSECURITY | INFRASTRUCTURE SECURITY | EMERGENCY COMMUNICATIONS | NATIONAL RISK MANAGEMENT | ABOUT CISA | MEDIA

Infrastructure Security > Chemical Security > Chemical Facility Anti-Terrorism Standards

Chemical Security

Chemical Facility Anti-Terrorism Standards
Ammonium Nitrate Security Program
Chemical Sector Security Events
Chemical Sector Resources

Chemical Facility Anti-Terrorism Standards

CFATS Laws and Regulations
Appendix A: Chemicals of Interest
Risk-Based Performance Standards

CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)

CFATS is the Nation's first regulatory program focused specifically on security at high-risk chemical facilities. The Cybersecurity and Infrastructure Security Agency (CISA) manages the CFATS program by working with facilities to ensure they have security measures in place to reduce the risks associated with certain hazardous chemicals, and prevent them from being exploited in a terrorist attack.

Follow @CISAgov and @CISAHarrell on Twitter for the latest infrastructure security news.

CFATS Announcements

- October 5, 2019: CISA published the CFATS Advisory Opinion 2019-001 on the Top-Screen reporting of theft/diversion mixtures that contain chemicals of interest (COI). To learn more, visit the CFATS Advisory Opinions page.
- July 9, 2019: CISA published a *Federal Register notice* announcing implementation of the CFATS Personnel Surety Program (PSP) at all high-risk chemical facilities—including Tier 3 and 4 facilities—closing the final gap to vet individuals with access to critical assets/restricted areas for terrorist ties. For more details, the PSP Toolkit, and a demo video, visit the PSP page.

Available Resources

Outreach: DHS outreach for CFATS is a continuous effort to educate stakeholders on the program.

- To request a CFATS presentation or a CAV, submit a request through the program website www.cisa.gov/cfats, or email DHS at CFATS@hq.dhs.gov

CFATS Help Desk: Direct questions about the CFATS program to the CFATS Help Desk.

- Hours of Operation are Mon. – Fri. 8:30 AM – 5:00 PM (ET)
- CFATS Help Desk toll-free number 1-866-323-2957
- CFATS Help Desk email address csat@dhs.gov

CFATS Web Site: For CFATS Frequently Asked Questions (FAQs), CVI training, and other useful CFATS-related information, please go to www.cisa.gov/cfats


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY