



***DHS
Chemical Facility
Anti-Terrorism Standards
(CFATS)
Summary***

Kort Dickson
Director, Corporate Security

CFATS - explained

- DHS rolled out in 2008-2010
- Meant to identify and provide standard for protecting our 'chemical facilities'
- Includes standards and chemical definitions
- Covered Chemicals (COI) listed with Quantity / Concentration and by 'hazard' (300+)
- Companies review inventory and register
- Perdue completed in 2009
- DHS rolled out CSAT 2.0 (updated version) in 2017

65422 Federal Register Vol. 72, No. 223 / Tuesday, November 20, 2007 / Rules and Regulations

Appendix A to Part 27. -- DHS Chemicals of Interest ¹

Chemicals of Interest (COI)	Synonym	Chemical Abstract Service (CAS) #	Release		Theft		Sabotage		Security Issue						
			Minimum Concentration (%)	Screening Threshold Quantities (in pounds)	Minimum Concentration (%)	Screening Threshold Quantities (in pounds unless otherwise noted)	Minimum Concentration (%)	Screening Threshold Quantities	Release - Toxic	Release - Flammables	Release - Explosives	Theft - CWC/DFP	Theft - WMD	Theft - EXP/EDP	Sabotage/Contamination
Ammonium nitrate, solid (nitrogen concentration of 23% nitrogen or greater)		6484-52-2			33.00	2000									X
Ammonium perchlorate		7790-98-9	ACG	5,000	ACG	400					X				X
Ammonium picrate		131-74-8	ACG	5,000	ACG	400					X				X
Amyltrichlorosilane		107-72-2						ACG	APA						X
Antimony pentasulfide		7783-70-2						ACG	APA						X
Arsenic trichloride	(Arsenous trichloride)	7784-34-1	1.00	15,000	30.00	2.2			X		X				
Arsine		7784-42-1	1.00	1,000	0.67	15			X			X			
Barium azide		18810-58-7	ACG	5,000	ACG	400					X			X	
1,4-Bis(2-chloroethylthio)-n-butane		142868-93-7			CUM	100g					X				
Bis(2-chloroethylthio)methane		63868-13-6			CUM	100g					X				
Bis(2-chloroethylthio)methyl ether		63918-90-1			CUM	100g					X				
1,5-Bis(2-chloroethylthio)-n-pentane		142868-94-8			CUM	100g					X				
1,3-Bis(2-chloroethylthio)-n-propane		63905-10-2			CUM	100g					X				
Boron tribromide		10294-33-4			12.67	45	ACG	APA					X	X	
Boron trichloride	(Borane, trichloro)	10294-34-5	1.00	5,000	84.70	45			X				X		
Boron trifluoride	(Borane, trifluoro)	7637-07-2	1.00	5,000	26.87	45			X				X		
Boron trifluoride compound with methyl ether (1:1)	(Boron, trifluoro (oxybis (methane))-T-4-)	353-42-4	1.00	15,000						X					
Bromine		7725-95-6	1.00	10,000					X						
Bromine chloride		13863-41-7			9.67	45							X		
Bromine pentafluoride		7789-30-2					ACG	APA						X	
Bromine trifluoride		7787-71-5			6.00	45	ACG	APA						X	
Bromotrifluoroethylene	(Ethene, bromotrifluoro-)	598-73-2	1.00	10,000					X						



CFATS Process / Steps-2017 forward

1. Re-Registration CSAT 2.0
2. Assignment of tiered ratings by DHS
3. Submit SVA's, SSP's or ASP's for High Risk sites
4. Complete Site Audits / Visits
5. Re-Certify / Monitor and Report

*Requires DHS
review and
approval*

Homeland Security **ISCD Portal**
Securing our Nation!

Disclaimer
You are about to access a Department of Homeland Security computer system. The computer system and data therein are property of the U.S. Government and are provided for official U.S. Government use only. There is no warranty or guarantee of any kind for the use of this computer system. The use of a password or any other security measure does not constitute an expectation of privacy. By using this system, you consent to the terms set forth in this notice. You may not provide, transmit, receive, or store information on this computer system. Access to this system is restricted to authorized users only. Unauthorized access, use, or modification of the system or of data contained therein, or in transit within this system, may constitute a violation of the laws of the U.S. Code and other federal laws. Anyone who discloses a Federal computer system without authorization or requests access, knowingly or otherwise, commits a crime, including, but not limited to, unauthorized access, use, or modification of the system or of data contained therein, or in transit within this system, may be subject to penalties, fines, or imprisonment. The computer system and any related equipment is subject to monitoring by administrative oversight. See Department of Homeland Security policies, procedures, and instructions for more information on proper performance of computer system security measures and procedures. This may restrict voluntary activities without further notice.

LOG IN WITH PIV AUTHORIZATION

LOG IN

LOG IN WITH TWO-FACTOR AUTHENTICATION

You are required to enter a valid Username/Password combination to proceed.

username

password

[Manage passwords...](#)

Unable to authenticate your account using the credentials provided or your account may be locked or disabled. If you have forgotten your password, click the [Forgot Password](#) link to reset your password and unlock your account. If you suspect your account is disabled, contact the ISCD Portal helpdesk using the information below.

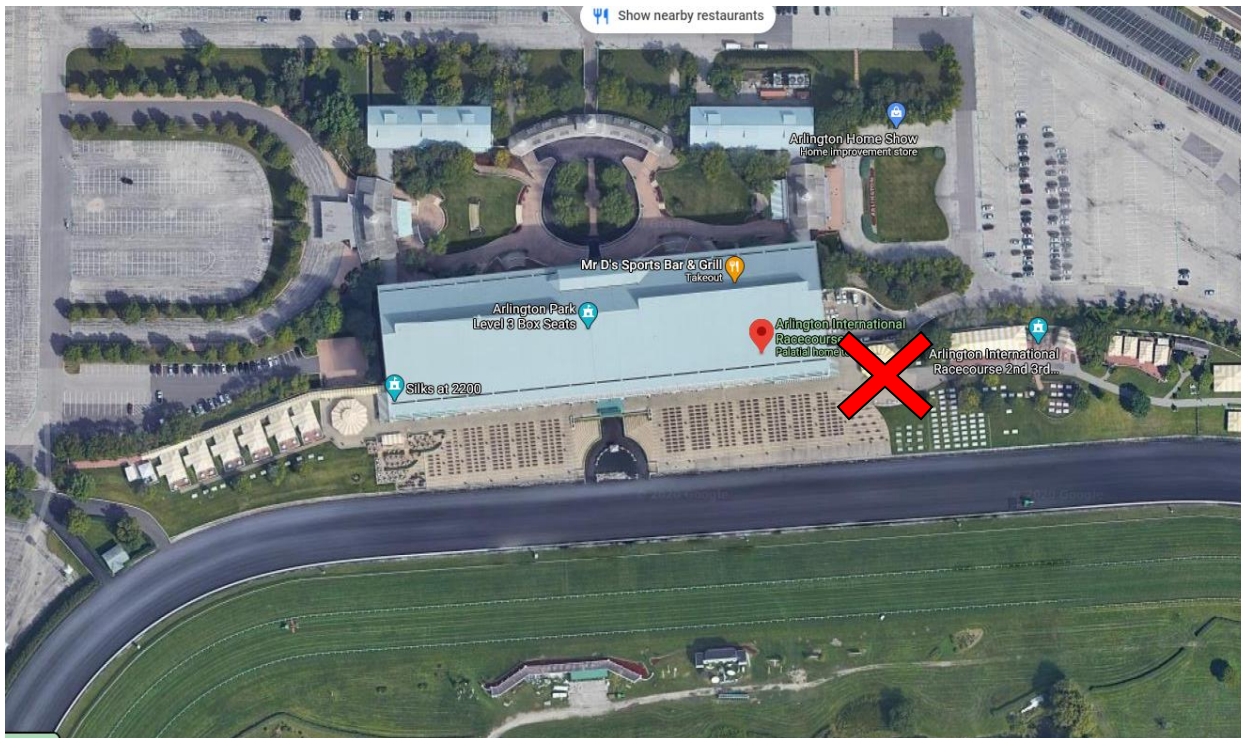
[Click here](#) to restart the login process.

Need Help?
[ISCD Portal Help Desk](#)
[ISCD Portal Privacy Policy](#)



CSAT 2.0 Online

1. Site info
2. Chemical holdings
3. Maps (site and covered chemicals)



Site Security Plans (compliance)

- 19 performance standards set forth

- | | |
|------------------------------|---|
| 1. Restrict Area Perimeter | 11. Conduct Training |
| 2. Secure Site Assets | 12. Personal Surety |
| 3. Screen and control access | 13. Elevated Threat response |
| 4. Deter, Detect, Delay | 14. Specific Threat response |
| 5. Shipping/Receipt/Storage | 15. Reporting (significant incidents) |
| 6. Theft / Diversion | 16. Tracking/Reporting Incidents/Activity |
| 7. Sabotage | 17. Organization to support |
| 8. Deter Cyber Sabotage | 18. Records maintenance |
| 9. Emergency Response | 19. Other (additions from Asst Secretary) |
| 10. Monitoring / Maintenance | |

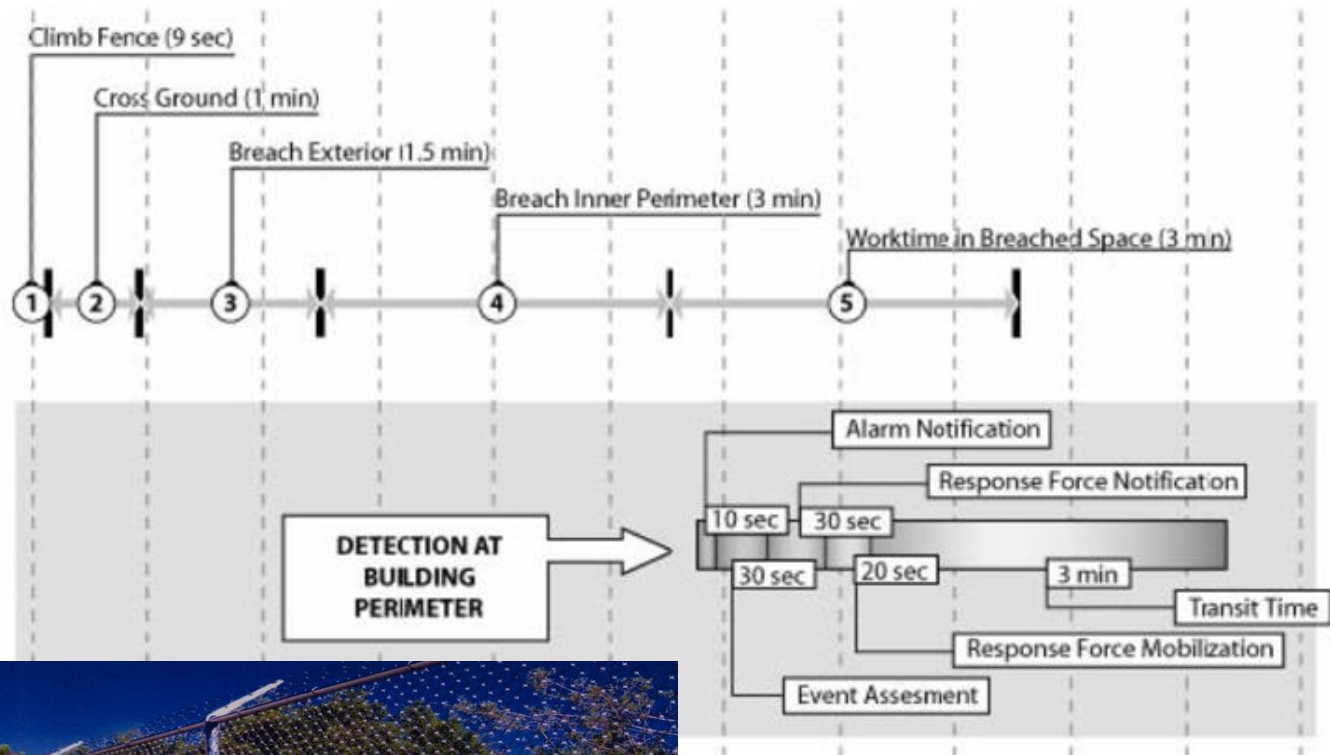
**.....All are covered by CVI or Chemical-Terrorism
Vulnerability Information regulations**



Barrier Performance – RBPS 4

Figure 1 – Barriers/Detection Performance

CFATS-Risk-Based-Performance-Standards-508



Shipping, Receipt, and Storage

Table 7: RBPS Metrics – RBPS 5 – Shipping, Receipt, and Storage

RBPS 5 - Shipping, Receipt, and Storage - Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility.

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials that make it extremely unlikely that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials that make it unlikely that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	The facility has documented processes for securing and monitoring the shipment, receipt, and storage of hazardous materials that reduce the likelihood that such materials would be made available to an unauthorized individual or an individual without a legitimate use for the material.	
Metric 5.1 – Security of Transportation Containers On-site	The facility adequately secures all transportation containers of hazardous materials on-site that are used for storage and are not incident to transportation, including transportation containers connected to equipment at a facility for loading or unloading and transportation containers detached from the motive power (e.g., a locomotive, truck/tractor) that delivered the container to the facility. Effective security generally includes storing the container within the facility’s security perimeter and under the facility’s security control, considering the container in the facility’s SSP, and securing and monitoring rail cars and other containers by using measures consistent with the materials that they contain.			
Metric 5.2 – “Know-Your-Customer” Provisions	The facility has an active, documented “know your customer” program that may include a policy of refusing to sell hazardous materials to those who do not meet pre-established customer qualification criteria, such as confirmation of identity, verification and/or evaluation of on-site security, verification that shipping addresses are valid business locations, confirmation of financial status, establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales), and verification of product end-use.			The facility has a “know your customer” program.
Metric 5.3 – Carrier and Shipment Facility Access	The facility has strict vehicle identification and entry authorization, shipping, and control procedures that are subject to a testing program to confirm reliability. If an unknown carrier arrives at the facility, the vehicle and its driver are staged until both the driver and the load are vetted and approved.			The facility has vehicle identification and entry authorization, shipping, and control procedures.

Training

Table 15: RBPS Metrics – RBPS 11 – Training				
RBPS 11 - Training – Ensure proper security training, exercises, and drills of facility personnel.				
	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility has a security awareness and training program for all facility personnel that includes drills and exercises designed to test and improve performance of aspects of the Site Security Plan and its supporting implementing procedures.			
Metric 11.1 – Security Training Program for Security Personnel	<p>The facility has a documented security awareness and training program and a corresponding set of minimum skills and competencies for security personnel, as well as a testing program through which security personnel can demonstrate their ability to perform their security-related tasks in a reliable and effective manner. A typical training program will include such features as:</p> <ul style="list-style-type: none"> • Training is provided on recognition of a security incident, reporting of a security incident, emergency procedures, and operation of security equipment. • Training is held on a regular basis for security personnel. • Objectives are established for each element of the training plan. • Training records are maintained in accordance with 6 CFR § 27.255(a)(1). 			
Metric 11.2 – Security Training Program for Non-Security Personnel	<p>The facility has a documented security awareness and training program for employees and resident contractors who do not have direct security responsibilities, and a testing program through which these employees and resident contractors can demonstrate their understanding of their roles in security. A typical training program will include features such as:</p> <ul style="list-style-type: none"> • Training provided on recognition of a security incident, reporting of a security incident, emergency procedures, and operation of security equipment. • Training is held on a regular basis for employees and resident contractors who do not have direct security responsibilities. • Objectives are established for each element of the training plan. • Training records are maintained in accordance with 6 CFR § 27.255(a)(1). 			
Metric 11.3 – Drills and Exercises	The facility plans and conducts security drills and exercises, which are documented and reviewed for lessons learned, on a periodic basis.			



Elevated Threats

Table 18: RBPS Metrics – RBPS 13 – Elevated Threats

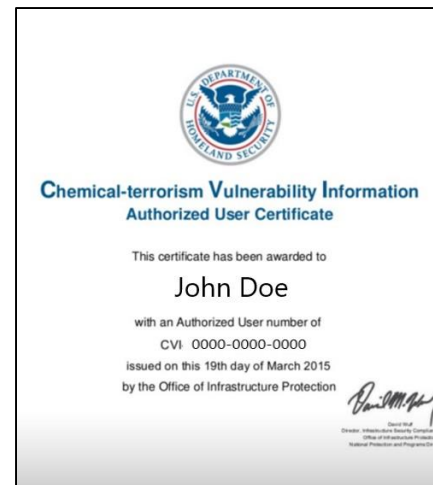
RBPS 13 - Elevated Threats - Escalate the level of protective measures for periods of elevated threat.

	Tier 1	Tier 2	Tier 3	Tier 4
Summary	The facility has a documented process for rapidly implementing an increased security posture in response to the elevation of the DHS HSAS threat level and has the ability to carry out that process in a timely manner.			
Metric 13.1 – Procedures	The facility has a written process and procedures for implementing security measures and increasing its security posture during periods of elevated threat to levels commensurate with the elevated threat. These security measures are specified and described in the SSP and tied to the HSAS threat level established by DHS.			
Metric 13.2 – Time Limits	The facility can very quickly achieve the security measures associated with each respective increased HSAS threat level while maintaining the measures already in use during normal operating periods.	The facility can quickly achieve the security measures associated with each respective increased HSAS threat level while maintaining the measures already in use during normal operating periods.		The facility can achieve the security measures associated with each respective increased HSAS threat level in a reasonable time period while maintaining the measures already in use during normal operating periods.



Basic Needs / Process

- *Program requires*
 - *Ongoing chemical holdings monitoring*
 - *Identification of a site FSO and AFSO*
 - *CVI Certification of all those 'with access to', 'with responsibility over' either the Plan or the Covered Chemical(s)*
 - *Annual 3rd party Audits of process, holdings, reports, etc.*
 - *DHS inspection every 18 months, to review site against submitted SSP*
 - *Extended Personnel Surety compliance – submitting all those with access, etc. to DHS*
 - *Documentation of All 18 RBPS's*




Cost implications?

- **Consultant Support**
 - *Individual site visits for each covered location for 3rd party audit and presence for DHS Audits*
 - *'Material modifications' to chemical inventory*
 - *Physical security enhancements*
- **Legal / Attorney review for approvals and general support**
- **Capital costs for;**
 - *'Material modifications' to chemical inventory*
 - *Physical security enhancements*
- **Non-Capital / Headcount for;**
 - *Security officer / support for ongoing regulatory compliance, monitoring, plan documentation and more.*





Questions?





[COVID Questions](#)


[Report Cyber Issue](#)


 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](#)

[Risk-Based Performance Standards](#)

[Appendix A: Chemicals of Interest](#)


[Chemical Security Assessment](#)

CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)

Original release date: July 06, 2009 | Last revised: July 31, 2020

CFATS is the nation's first regulatory program focused specifically on security at high-risk chemical facilities. Managed by the Cybersecurity and Infrastructure Security Agency (CISA), the CFATS program identifies and regulates high-risk facilities to ensure they have security measures in place to reduce the risk that certain hazardous chemicals are weaponized by terrorists.

Follow [@CISAgov](#) and [@CISAHarrell](#) on Twitter for the latest infrastructure security news.



CFATS Announcements

- July 22, 2020: The President signed into law [Pub. L. No. 116-150](#) to extend the expiration date of the *Protecting and Security Chemical Facilities from Terrorist Attacks Act of 2014*, Pub. L. No. 113-254, to July 27, 2023.
- 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](#).

[Expand All Sections](#)

CFATS Overview

