

Frequently Asked Questions About the Chemical Facility Anti-Terrorism Standards (CFATS)

AcuTech Consulting Group
McLean, VA
www.acutech-consulting.com

Industry and government agencies recognize AcuTech as a leader in chemical security and vulnerability assessment. We have assisted industry in conducting SVAs and developing SSPs at a wide variety of chemical facilities in the US and abroad. AcuTech staff includes recognized experts with both industry and government security experience. Following is a series of Questions & Answers that AcuTech clients might find helpful as they strategize their compliance efforts. **This Q&A document is for information only.**

What is CFATS?

As part of the Homeland Security Appropriations Act of 2007 (Pub. Law 109-295), Sec. 550), Congress directed the Department of Homeland Security (DHS) to identify and regulate “high risk chemical facilities.” The new Chemical Facility Anti-terrorism Standard (CFATS) went into effect on June 8, 2007 pursuant to an Interim Final Regulation (IFR) that was published in the Federal Register on April 9, 2007 (72 Fed Reg 17688). The new rules, promulgated as 6 CFR Part 27 will allow DHS to identify high risk chemical facilities, require such facilities to conduct a Security Vulnerability Assessment (SVA) and prepare a Site Security Plan (SSP) that reflects risk-based performance standards (RBPS) established by DHS.

There are several notable characteristics of this new program:

- CFATS is *risk-based* -- DHS will assign high risk facilities to one of four tiers and will impose requirements and standards based on the potential risk represented by the different tiers.
- CFATS is *performance-based* – rather than prescribing specific security measures for all facilities, or even for all facilities in a given tier, it establishes risk based performance standards (RBPS) that will allow a facility to implement security measures that, taken together, meet the applicable RBPS for its tier.
- CFATS *builds on existing industry voluntary effort and investments* – following 9/11, facilities throughout the chemical sector developed security programs and initiatives to reduce the vulnerabilities to terrorist attacks. Some companies and facilities developed and implemented their own programs while others participated in broader industry initiatives such as the American Chemistry Council’s Responsible Care[®] Security Code or the American Petroleum Institute’s “Security Guidelines.” Many facilities conducted vulnerability assessments using methodologies developed by Sandia National Labs, the Center for Chemical Process Safety, or other methodologies derived from those two methods.

How do I know if my facility is affected?

Unlike many EHS-related regulations (e.g., PSM, RMP), the requirements of CFATS are not triggered solely by having certain chemical(s) onsite above a threshold. Because CFATS is risk-based, coverage by the regulations is determined by the consequences of the abuse/misuse of certain chemicals. About 300 chemicals are included in CFATS as “chemicals of interest” (listed in Appendix A to the IFR). Those sites possessing more than the screening threshold quantity (STQ) of one or more of these chemicals must perform an online screening analysis. The results of this screening will determine whether the site is subject to the remaining provisions of the regulation and the preliminary tier level. The CFATS regulation also includes several statutory exemptions. Subsequent information gathering and assessment efforts, largely through the conduct of an SVA, will allow DHS to finalize the tier level assigned to each site and its assets. These sites will then be required to meet the risk-based performance standards (RBPS) with layered security measures that represent increasing rigor with higher tiered sites.

Facilities that are **not** included in the regulated community may include the following groups:

- Those facilities regulated pursuant to the Maritime Transportation Security Act (MTSA) of 2002; facilities owned or operated by the Department of Defense, the Department of Energy and those subject to significant regulation by the Nuclear Regulatory Commission (those with small radioactive sources are not exempt); Public Water Systems as defined by section 1401 of the Safe Drinking Water Act; Treatment Works as defined in Section 212 of the Federal Water Pollution Control Act;
- Facilities that possess chemicals on the DHS list of Chemical of Interest, but *below* the STQ;
- Facilities that are not considered “high risk” after CFATS screening.
- Facilities that possess listed chemicals, but whose activities are not included in the scope of CFATS by policy (e.g., rail yards were mentioned in the preamble to the interim final rule).

Where do I find the list of chemicals that will tell me if I have to use the online screening tool?

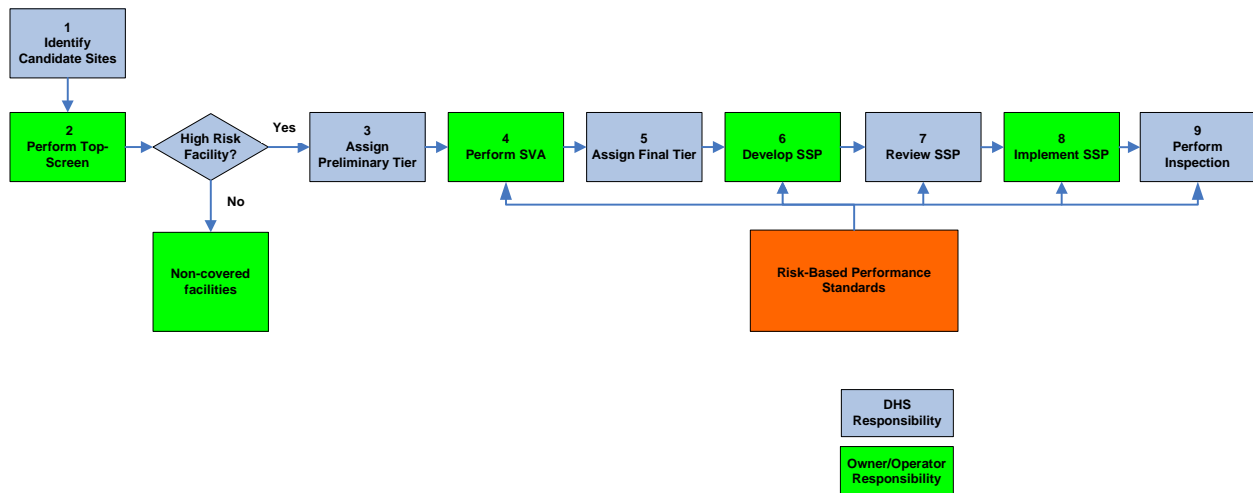
The list of about 300 DHS Chemicals of Interest (COI) may be found in Appendix A to the IFR (6 CFR Part 27). The list of chemicals is critical to determining what actions facilities should take. If a facility possesses any of the chemicals on the list at or above the STQ (which is specific to each chemical), the facility must register to use the Chemical Security Assessment Tools and submit a Top-Screen to DHS. Instructions for determining whether a facility meets the STQ for a particular chemical (including the appropriate considerations for chemicals in a mixture) are found in the Appendix A list rule to be published in the Federal Register on or about November 16, 2007. Possession of a chemical on Appendix A at or above the STQ triggers the requirement for a facility to submit a Top-Screen; it does not necessarily mean that the facility is “in” or “out” of CFATS.

What does the CFATS process look like?

CFATS creates a system composed of discrete elements that, taken together, constitute a progressive program to identify high risk chemical facilities and to impose security standards commensurate with the security risk profile of such covered facilities. DHS developed an online process for registering facilities, screening, SVA, and SSP submittal named the Chemical Security Assessment Tool (CSAT).

Figure 1 describes the general sequence of the key regulatory requirements and milestones.

Figure 1 - Strategic Approach CFATS



- Facilities manufacturing, storing, or using “*Chemicals of Interest*” at or above STQ will first complete a “*Top-Screen*” accessible through a secure Department web application (CSAT) available at www.dhs.gov/chemsecurity.
- Facilities that meet security risk thresholds determined by DHS’s analysis of the Top-Screen information will be assigned a preliminary tier level and will be requested in writing to submit an online CSAT Security Vulnerability Assessment (SVA).
- Results of the SVA will determine the final tier level and facilities in Tiers 1-4 will be requested in writing to complete an online Site Security Plan (SSP) where the site will describe its current and planned security measures to achieve the applicable *Risk Based Performance Standards (RBPS)* which are scalable according to the facility’s risk tier.
- A covered facility’s SSP will be approved by DHS *and* will be used during enforcement of the regulation.

What kind of issues is DHS concerned about at these high risk facilities?

DHS is collecting information and assessing facilities based on several security issues or groups of issues:

- Risk to public health and safety from a release of:
 - toxics chemicals
 - flammable chemicals
 - explosive chemicals

- Risk to public health and safety from theft or diversion of:
 - Chemical weapons and precursors with “bathtub chemistry” potential
 - Weapons of mass effect (toxic inhalation gases that can be used as weapons directly)
 - Improvised Explosive Device (IED) Precursors

- Risk to public health and safety from sabotage or contamination of materials that could release toxic inhalation gases if exposed to water

DHS is also collecting information on two additional security issues, but will not tier facilities based on this information at this time:

- Risks to the ability of the government to provide critical services in the event of an emergency with:
 - Public health
 - Potable drinking water and electric power
 - National defense

- Risks to the national or regional economy

What is the timing of CFATS-related activities?

Once Appendix A has been published, facilities have 60 days to submit their Top-Screen questionnaires.¹ DHS intends to respond to submitters regarding their preliminary tier assignment within another 60 days. Facilities assigned to Tiers 1-3 will have 90 days to complete a CSAT SVA which DHS will review within 60 more days [Tier 4 sites may submit an Alternate Security Program in lieu of a CSAT SVA]. Once DHS has communicated to facilities regarding their final tier assignment and the appropriateness of their SVA, facilities will have 120 days to complete and submit an SSP to DHS. DHS will inspect covered facilities to insure the implementation of the SSP and issue a Letter of Authorization if it is approved.

Facilities assigned to Tiers 1 and 2 must update their Top-Screen, SVA, and SSP every two years while facilities assigned to Tiers 3 and 4 are on a three-year schedule.

¹ Facilities must submit a Top-Screen if they possess any chemical listed on Appendix A at or above the STQ. If a facility later comes into possession (*plans* to possess) of a chemical listed on Appendix A at or above the STQ, the facility has 60 days to notify DHS and submit a Top-Screen for that chemical.

What are Risk-Based Performance Standards (RBPS)?

CFATS includes 19 categories of Risk-Based Performance Standards (RBPS) [see Attachment A for a brief list of the RBPS]. The standards are scalable meaning that facilities at higher tiers will be required to meet tougher risk-based standards than facilities assigned to lower tiers. Congress explicitly prohibited DHS from imposing specific measures or disapproving an SSP because it lacks a specific measure. The risk-based approach is intended to be flexible and to state a security outcome or goal, thereby allowing facilities the choice of how to achieve that outcome or goal.

DHS has recently published draft guidance on how the RBPS may be applied across the 4 tiers. While changes may be made to the text of the guidance before it is finalized, it is now possible to have an excellent idea of how DHS expects facilities at different tiers to comply with the RBPS and document compliance through the Site Security Plan. The draft guidance is available at www.dhs.gov/chemicalsecurity.

What if I already did an SVA and have an SSP?

Facilities that are assigned to Tiers 1-3 must use the CSAT SVA tool. The use of the CSAT SVA is not strictly required for a Tier 4 facility. Tier 4 facilities may submit for review and approval the Sandia RAM for chemical facilities, the CCPS SVA Methodology for fixed chemical facilities, or any methodology certified by CCPS as equivalent to CCPS as described by DHS in the IFR. Facilities in Tiers 1-3 may submit an Alternative Security Plan in lieu of a SSP.

How is information submitted to DHS protected?

DHS has included provisions in the CFATS regulation to protect from public disclosure extremely sensitive information that facilities develop for purposes of complying with the CFATS. They balance the need to protect the information with the need to share relevant information with state and local government officials who have a "need to know" to carry out chemical facility security activities. To have access to Chemical-terrorism Vulnerability Information (CVI), individuals with a "need to know" will need to take DHS' online training and comply with the CVI requirements.

Where are we in the process now?

Generally speaking, most facilities have submitted their Top-Screens and been sent an initial notification of high-risk and tier letter. This letter informed the facility about the COI and security issues of concern to DHS and required each "high risk" facility to submit a CSAT SVA (or ASP for Tier 4 facilities meeting the requirements) by a certain date. The facilities that submitted SVAs are now awaiting a Final Tier Notification. Tier 1 facilities should expect to hear from DHS in January 2009; Tier 2 in February 2009; Tier 3 in early summer; and Tier 4 sometime after that. The Final Tier Notification letter will outline the requirements and deadlines for the Site Security Plan that will be required to document compliance with the RBPS.

What should I do to get ready now?

It is important that each facility be ready to engage in the next step of the CFATS process as the deadlines are strict. Here are some things you can do now to prepare:

- Review the draft Risk-Based Performance Standards on the DHS Chemical Security website.
- Review the SVA you submitted to DHS and consider gaps you may have noticed during the SVA process. Unless you feel your facility's tier will change, you can make some educated guesses as to what measures and metrics will apply to your facility.
- Consider what kinds of security training your facility will need.
- Consider how and whether security procedures already in place or newly required (such as the new TSA Rail Security rule) will be coordinated and reflected in your SSP.
- Consider where and how you will collect and maintain documentation for CFATS compliance (RBPS 18-Records)
- Maintain your knowledge of CVI procedures. DHS recently reissued the CVI procedures manual and several requirements have changed.
- Consider how you will prepare for a DHS inspections. Facilities at higher tiers can expect inspections sooner.

For more information

Contact AcuTech Consulting Group for expert advice, training and assistance at (703) 245-3015 or help@acutech-consulting.com.

Attachment A: Risk-Based Performance Standards

Section 27.230 Risk-Based Performance Standards

- (1) **Restrict Area Perimeter.** Secure and monitor the perimeter of the facility;
- (2) **Secure Site Assets.** Secure and monitor restricted areas or potentially critical targets within the facility;
- (3) **Screen and Control Access.** Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,
 - (i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and
 - (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;
- (4) **Deter, Detect, and Delay.** Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:
 - (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;
 - (ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;
 - (iii) Detect attacks at early stages, through counter-surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and
 - (iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning.
- (5) **Shipping, Receipt, and Storage.** Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;
- (6) **Theft and Diversion.** Deter theft or diversion of potentially dangerous chemicals;
- (7) **Sabotage.** Deter insider sabotage;
- (8) **Cyber.** Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems;
- (9) **Response.** Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;
- (10) **Monitoring.** Maintain effective monitoring, communications and warning systems, including
 - (i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;
 - (ii) Measures designed to regularly test security systems, note deficiencies, correct for

Section 27.230 Risk-Based Performance Standards

- detected deficiencies, and record results so that they are available for inspection by the Department; and
- (iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;
- (11) Training.** Ensure proper security training, exercises, and drills of facility personnel;
- (12) Personnel Surety.** Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,
- (i) measures designed to verify and validate identity;
 - (ii) measures designed to check criminal history;
 - (iii) measures designed to verify and validate legal authorization to work; and
 - (iv) measures designed to identify people with terrorist ties;
- (13) Elevated Threats.** Escalate the level of protective measures for periods of elevated threat;
- (14) Specific Threats, Vulnerabilities, or Risks.** Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;
- (15) Reporting of Significant Security Incidents.** Report significant security incidents to the Department and to local law enforcement officials;
- (16) Significant Security Incidents and Suspicious Activities.** Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;
- (17) Officials and Organization.** Establish official(s) and an organization responsible for security and for compliance with these standards;
- (18) Records.** Maintain appropriate records; and
- (19) Address any additional performance standards** the Assistant Secretary may specify.