



**CISA**  
CYBER+INFRASTRUCTURE

## **Guidance Document**

**The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.**

Document Summary: The following document interprets relevant regulations and concludes that background checks are required for all employees of covered chemical facilities with access to chemicals of interest. It specifies that there is no exclusion or exemption for employees who had access to chemicals of interest prior to the implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) regulations.

Document Title: RBPS-12 Background Check Requirements for Legacy Employees

Issued by: Infrastructure Security Compliance Division, Cybersecurity and Infrastructure Security Agency

Date of Issuance/Revision: October 5, 2016

Affected parties: Facilities possessing mixtures of chemicals of interest (COIs) classified as theft/diversion COI.

Statutory or regulatory provisions interpreted: 6 CFR 27.230(a)(12)

Document Identification Number: CISA-ADV-2016-001

Link: [www.cisa.gov/publication/cfats-ao-2016-001](http://www.cisa.gov/publication/cfats-ao-2016-001)



Homeland  
Security

## CFATS ADVISORY OPINION 2016-001

**POSTED:** October 5, 2016

**TOPIC:** RBPS-12 Background Check Requirements for Legacy Employees

**ISSUE SUMMARY:** Under the Chemical Facility Anti-Terrorism Standards (CFATS), 6 C.F.R. part 27, covered chemical facilities must ensure that background checks are conducted on certain individuals with or seeking access to their restricted areas or critical assets. See 6 C.F.R. § 27.230(a)(12). The attached letter addresses the requirement to conduct these background checks on legacy/long-time employees in addition to conducting them on newer employees. The Department of Homeland Security's longstanding position and interpretation of 6 C.F.R. § 27.230(a)(12) is that background checks are required to be conducted for all facility personnel with access to restricted areas or critical assets at high-risk chemical facilities, regardless of their length of service, as described in more detail in the attachment.

**ATTACHMENT:** Letter from the Infrastructure Security Compliance Division to a Chemical Facility Representative, dated May 23, 2016 (Redacted)

*We redact Chemical-terrorism Vulnerability Information (CVI), identifying information, and other potentially privileged, confidential, or propriety information from CFATS Advisory Opinion postings.*



Homeland  
Security

May 23, 2016

[REDACTED]

Dear [REDACTED],

The Infrastructure Security Compliance Division (ISCD), of the U.S. Department of Homeland Security, is sending you this letter to confirm direction that we have provided to [REDACTED] regarding the requirement to conduct certain types of background checks on legacy employees at [REDACTED].

As ISCD has previously conveyed to [REDACTED], [REDACTED] site has been determined to be a high-risk chemical facility pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS), 6 C.F.R. part 27. The [REDACTED] site is therefore a covered chemical facility, regulated under CFATS. As such, the facility is required (under CFATS) to draft and, after approval by ISCD, implement a Site Security Plan (SSP). The facility's SSP was approved last year, and the facility is obligated by CFATS to implement and comply with its SSP.

Risk-Based Performance Standard #12 of CFATS requires that each high-risk chemical facility include the following in its SSP:

- Measures designed to verify and validate identity of all facility personnel and unescorted visitors with access to restricted areas or critical assets;
- Measures designed to check criminal history of all facility personnel and unescorted visitors with access to restricted areas or critical assets;
- Measures designed to verify and validate legal authorization to work of all facility personnel and unescorted visitors with access to restricted areas or critical assets; and
- Measures designed to identify individuals with terrorist ties as to all facility personnel and unescorted visitors with access to restricted areas or critical assets.<sup>1</sup>

<sup>1</sup> 6 C.F.R. § 27.230(a)(12). See also 6 U.S.C. § 622(a)(2)(D)(ii) (portion of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 – the statutory basis for CFATS – requiring high-risk chemical facilities to implement SSPs after development).

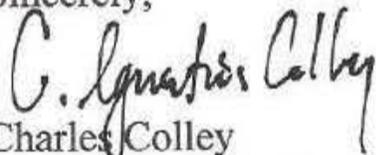
Although ISCD does not yet have the authorization (pursuant to the Paperwork Reduction Act) to process terrorist ties checks for facilities of the [REDACTED] risk tier level,<sup>2</sup> the facility is required to conduct all three other types of background checks on all of its facility personnel and unescorted visitors with access to restricted areas or critical assets on site. Identity checks, criminal history checks, and legal authorization to work checks are requirements of both 6 C.F.R. § 27.230(a)(12) and the facility's approved SSP. These three types of background checks are required for legacy employees.

Under CFATS, facility personnel with access to restricted areas or critical assets are not exempt from the background check requirements listed above due to length of service, status as prior employees of a facility or business that has been acquired by a high-risk chemical facility, or any other factor. The preamble to the CFATS Interim Final Rule clearly states that long-time employees are not exempt from background check requirements. In drafting the Interim Final Rule, the Department of Homeland Security explicitly rejected comments suggesting that long-time employees should be "grandfathered" and exempt from background checks under CFATS, and stated the following:

The rule does not include a provision that would exempt certain employees from the personnel surety performance standard based on length of employment at the facility. Merely because an individual has worked in a chemical facility for a period of time without incident does not automatically mean that they do not pose a terrorism risk and should be given free access to restricted areas and critical assets without a background check. Allowing such access without a background check presents an unacceptable security risk, and is contrary to the performance standard on personnel surety.<sup>3</sup>

Accordingly, [REDACTED] must conduct background checks on all facility personnel with access to restricted areas or critical assets at the [REDACTED] site, regardless of length of service. It is ISCD's longstanding position that background checks for all facility personnel with access to restricted areas or critical assets are essential to a sufficient SSP. [REDACTED] must complete them in accordance with any timelines for completion listed in its SSP.

Sincerely,

  
Charles Colley  
Branch Chief for Compliance (Acting)  
Infrastructure Security Compliance Division  
Office of Infrastructure Protection  
U.S. Department of Homeland Security

<sup>2</sup> ISCD will notify facilities of the [REDACTED] risk tier level at a later date if ISCD gains authorization to begin processing terrorist ties checks for facilities of that risk tier level. The [REDACTED] may be required to implement measures to conduct terrorist ties checks if that happens in the future. The facility is not required to implement measures to conduct terrorist ties checks in the interim.

<sup>3</sup> 72 F.R. 17687, 17708 (April 9, 2007).