AmericanCoatings
ASSOCIATION

June 4, 2013

Infrastructure Security Compliance Division
Office of Infrastructure Protection
National Protection and Programs Directorate
US Department of Homeland Security
Washington, DC 20528

RE: DHS-2012-00611, Information Collection Request: Chemical Facility Anti-Terrorism Standards Personnel Surety Program

To the CFATS Program Manager:

The American Coatings Association (ACA)[1] appreciates the opportunity to submit comments on the U.S. Department of Homeland Security's Information Collection Request (ICR); Chemical Facility Anti-Terrorism Standards Personnel Surety Program.[2] ACA's members own and operate paint, coatings, resin, and chemical manufacturing facilities that are subject to the provisions of the Chemical Facility Anti-Terrorism Standards (CFATS), and under CFATS's statutory authority, many ACA members have submitted top-screens identifying chemicals of interest and have been assigned preliminary or final tiers by the Department. As a result, these member companies have become subject to a myriad of CFATS requirements, including that of complying with Risk-Based Performance Standard 12 (RBPS-12), Personnel Surety. The present ICR constitutes the Department's effort to provide a means by which "high risk chemical facilities" may comply with RBPS-12.

Discussion

ACA, like many of its industry colleagues, believes the changes incorporated in this ICR are improvements over the initial, withdrawn draft,[3] and improve flexibility, increase efficiency and reduce burden for facilities. Among these improvements are the somewhat expanded use of existing Federal vetting programs, specifically the Transportation Worker Identification Credential (TWIC) Program and the

[1] The American Coatings Association (ACA) is a voluntary, nonprofit trade association working to advance the needs of the paint and coatings industry and the professionals who work in it. The organization represents paint and coatings manufacturers, raw materials suppliers, distributors, and technical professionals. ACA serves as an advocate and ally for members on legislative, regulatory and judicial issues, and provides forums for the advancement and promotion of the industry through educational and professional development services.
[2] 78 Fed. Reg. 17680 (March 22, 2013).
[3] 74 Fed. Reg. 27555

Hazardous Materials Endorsement (HME) Program as viable compliance options to validate personnel security information. DHS also states facilities may use "other technology that is periodically updated using the Cancelled Card List," in order to vet personnel that do not hold valid TWIC Cards. While this is a step forward, as noted hereinbelow, DHS could improve this and other provisions within this ICR to lessen the burden on regulated facilities.

According to the ICR, "the purpose of the CFATS Personnel Surety Program is to identify individuals with terrorist ties that have or are seeking access to the restricted areas and/or critical assets at the nation's high-risk chemical facilities."[4] DHS indicates that this requirement is imposed pursuant to Congressional authorization of the program in Section 550 of the DHS Appropriations Act of 2007, which required DHS to "establish risk-based performance standards for chemical facilities."[5] DHS subsequently enumerated 18 Risk-Based Performance Standards that covered chemical facilities must meet to be in compliance with CFATS.[6]

DHS addresses the concept of performance standards in its May 2009 guidance document, "Risk-Based Performance Standards Guidance," noting that "Performance standards" have a long and well-established history in Federal rulemakings. As the Office of Management and Budget has explained, performance standards "state[ ] requirements in terms of required results with criteria for verifying compliance but without stating the methods for achieving required results." Stated differently,

> A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal and lets each regulated entity decide how to meet it.[7]

The Guidance Document further provides extensive direction on the implementation of each Risk-Based Performance Standard, including RBPS-12, noting that

> …the primary means of satisfying the personnel surety performance standards is through the implementation of an appropriate background check program….In the context of CFATS RBPS 12, a background check is the process of acquiring information on an individual regarding the legal authority to work for a high-risk chemical facility, have access to its restricted areas, or for other activities that involve access to a restricted area or critical asset at a high-risk chemical facility. Background checks can range from simple employment screening (i.e., using public or commercially available records and investigation to confirm or disprove the accuracy of an applicant's resume)

[4] *Id*. at 17682.
[5] P.L. 109-295
[6] 6 C.F.R. §27.230.
[7] Office of Infrastructure Protection, Infrastructure Security Compliance Division, Department of Homeland Security, "Risk-Based Performance Standards Guidance," May 2009, at 10 (hereinafter cited as "RBPS Guidance Document"). The passage quoted above contains citations to Cary Coglianese et al., *Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection*, 55 Admin. L. Rev. 705, 706–07 (2003), as well as OMB Circular A-119 (Feb. 10, 1998).

> to comprehensive investigations that consider prior criminal activity, immigration status, credit checks, potential terrorist ties, and other, more in-depth analysis.[8]

In this Guidance Document, DHS does note that it is in the process of developing a system to have "relevant individuals screened by DHS through the Terrorist Screening Database (TSDB)"[9] -- a system which is now the subject of this ICR.

Despite Congressional intent that CFATS be implemented as a performance standard – an operating concept DHS acknowledged in its own description of risk-based performance standards -- the program as envisioned by DHS in this ICR is in practice quite prescriptive. As proposed, it not only provides little flexibility to the business needs of the affected facilities, but fails to adequately utilize other DHS programs and systems currently in place. In particular, it imposes a number of requirements that will be very difficult for affected facilities to meet while concurrently operating their primary business – specifically, the general requirement outlined in the ICR that a high-risk chemical facility submit information about individuals under Option 1 and/or Option 2 visitors' 48 hours prior to their having unescorted access to restricted areas or critical assets.[10]

Most coatings industry facilities that have been tiered under CFATS are so-called "theft and diversion" facilities, where the major security risk is the loss of a listed chemical of interest (COI) due to theft, pilferage, or purchase by someone impersonating a legitimate purchaser. The overwhelming majority of coatings manufacturing facilities that have received preliminary or final tier assignments have been designated as Tier 4, the lowest risk level. In the case of coatings manufacturers, the diversion of a COI through purchase is simply not plausible, since coatings manufacturers do not typically acquire commercial-grade chemicals of interest for re-sale for resale, but rather for use in formulated products, which are not themselves COIs even when they incorporate a COI raw material. A number of coatings facilities have proposed making the entire manufacturing footprint a secure area, since the process of coatings manufacture may make it infeasible to isolate a commonly used raw material to a specific secure location. The result of this is that the routine presence of delivery personnel, repair and maintenance personnel, etc. at a coatings manufacturing site would trigger the 48-hour requirement under the ICR – no matter how well-known these individuals might be to the plant manager.

Access control to affected facilities is directly governed by RBPS-3 ("Screen and Control Access"). It is instructive to view the issue of access control through the lens of RBPS-3 requirements. Specifically, the requirement to "Screen and Control Access" specifies, in the case of Tier 3 and 4 facilities, that "the facility has access control systems that provide for *reasonable identity verification*, such as the issuing of tamper-resistant ID badges to all facility employees, and the provision of visitor badges to, and *escorting or monitoring of*, all individuals without permanent ID badges."[11] This reasonable requirement is completely obviated by a considerably more onerous requirement in this ICR that not only must such visitors be escorted or monitored and have their identifies reasonably verified (as specified in RBPS-2), but that their names must also be submitted for screening against a DHS database no less than 48 hours prior to their arrival at the facility. DHS asserts that is "…does not believe that if a facility complies with RBPS

[8] *Id.* at 97.
[9] RBPS Guidance Document at p. 97.
[10] 78 Fed. Reg. at 17687.
[11] RBPS Guidance Document at p. 48.

12(iv) the high-risk chemical facility will, on a routine basis, experience an unreasonable impact in allowing affected individuals access to restricted areas or critical assets."[12] Industry is skeptical of this rosy view. *Even* if a coatings manufacturer is able to obtain the necessary personal identifying information required to make such a submission from a delivery company, waste hauler, etc., and *even* if DHS invariably is able to turn around such requests in this timeframe (something that experience tells us may be unlikely over weekends, holidays, etc.), there is considerable likelihood that this system will prove to be difficult or even unworkable in practice. DHS contends that this requirement's burden will be minimal because the data submission is likely to be accomplished in concert with the other routine hiring and access control involving background check described above."[13] This glosses over the problem of working with third parties, who are often small businesses, such as a contractor, haulers, etc. and being able to obtain from them this sort of data on their employees well in advance of a shipment or pick-up or emergency repair situation (or that they can even identify which of their employees will actually be the ones who are dispatched to the facility). Looking at the issue in this light suggests that the actual financial and operational burden will be substantially higher than DHS suggests.

ISCD appears to believe that the remedy to the issues raised by this 48-hour requirement is simply to provide escorts for all visitors. This apparent solution is, however, overly simplistic and is likely to be very problematic in practice. A small -- or even a large -- chemical facility may have a relatively small staff, all of whom are typically fully employed performing other important work elsewhere in the facility. Moreover, coatings and other chemical facilities frequently have a number of non-employee visitors on their sites – these may include repair personnel and other contractors, but more often involve transportation workers making deliveries and picking up product shipments, waste materials, mail, etc. to transport off-site. Requiring that regulated facilities assign an escort to every delivery vehicle that might visit a plant on a daily basis, or otherwise seeking to screen those individuals against the TSDB 48 hours prior to the need, simply fails to understand or accommodate the business realties facing these businesses. It is also not always feasible to limit the use of a COI to a small or specific and tightly controlled location, due to the exigencies of the production process.

As noted in the ICR, high-risk chemical facilities, or their parent companies, may choose to comply with RBPS 12(iv) by identifying and submitting the information about affected individuals to the Department directly. Alternatively, high-risk chemical facilities, or their parent companies, may choose to comply with RBPS 12(iv) by outsourcing the information submission process to third parties. In either case, these facilities will be collecting and transmitting considerable amounts of personally identifiable information (PII) on a number of employees and non-employee personnel.[14]

Although DHS somewhat acknowledges the burden of submitting data for multiple high-risk facilities, as well as the potential burden of submitting duplicate records about an affected individual, ACA believes that the Department substantially underestimates the burden and the potential liability this requirement

[12] 78 Fed. Reg. at 17684.
[13] *Id*.
[14] According to DHS guidance, "DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department." "Handbook for Safeguarding Sensitive PII at DHS," DHS Privacy Office (January 19, 2011) at p. 5.

places on affected facilities, particularly with respect to non-employee personnel. DHS, while alluding to the dangers associated with the collection and transmission of massive amounts of personally identifiable information (PII) to comply with the requirements contained in this ICR, largely glosses over the difficulties in dealing with PII:

High-risk chemical facilities, or their designees, are responsible for complying with the federal, state, and national privacy laws applicable to the jurisdictions in which they do business. The Department *believes* that high-risk chemical facilities, or their designees, have multiple, established legal avenues that enable them to submit PII to the Department, which may include the Safe Harbor Framework [reference omitted] and meet their privacy obligations (emphasis added).[15]

Among many issues raised by the ICR are not only those associated with the necessary collecting of sensitive PII from members of the public, such as employees or plant contractors or visitors, but also the related problems raised by the need to facilities to create a process to collect that sensitive PII. Does the collection of personal data from members of the public at the behest of DHS trigger any requirements under the Paperwork Reduction Act (PRA) or the Privacy Act? While DHS appears to envision the submission of these data using the Chemical Security Assessment Tool (CSAT) Personnel Surety application, this tool is unwieldy, involves a variety of roles, such as Preparer, Submitter, Authorizer and Reviewer, and requires training to be able to competently upload data.[16] In lieu of use of CSAT, would the information collected to implement this RBPS-12 requirement be transmitted by email or over the telephone if necessary to admit a visitor who cannot be escorted? Email systems do not currently qualify as secure systems and have instead been identified by OMB as 'general support systems' used to transmit information.

At a minimum, unless and until DHS can authoritatively prescribe how chemical facilities can safely collect this information and submit it to DHS without incurring possible legal liability, this ICR is fatally flawed and is not ready to be fielded and implemented by regulated entities (in the form of SSPs and ASPs). Again, these problems are particularly acute with non-employee visitors, for whom a facility would not otherwise collect or transmit PII. This area of holding PII is itself fraught with potential legal problems, which is why DHS should aim to minimize the need to collect and transmit data and maximize its reliance on other programs that accomplish largely the same aim as RBPS-12 (i.e., identity verification).

Along with our industry colleagues, ACA has asked ISCD to leverage the large number of DHS programs that have similar objectives and/or collect similar data elements in order to support implementation of CFATS, instead of duplicating these other DHS programs in an overly redundant way. In our observation, DHS often behaves as if its various sub-agencies not only are entirely unaffiliated, but as if they are entities of unrelated sovereigns. For example, the Form I-9 (Employment Eligibility Verification) issued by the U.S. Citizenship and Immigration Service (USCIS) – itself an operating agency within the Department of

[15] 78 Fed. Reg. at 17685.

[16] CSAT Guidance also indicates that the submitter be a corporate officer formally assigned to this role, which is an added hurdle, particularly with respect to infrequently present non-employee personnel. A "Submitter" is an individual certified by the company or corporation to formally submit the required regulatory data to DHS. To be a "Submitter," an individual must be an officer of the corporation—or be designated by an officer of the corporation—and must be domiciled in the United States. See *CSAT User Registration User Guide* at 3 (October 2011).

Homeland Security – solicits essentially the same information required under the direct vetting option identified in the ICR and is specifically alluded to in the context of RBPS-12(iii) ("Measures designed to verify and validate legal authorization to work"). Despite this, the ICR omits any mention of this specific data collection program operated by another arm of the DHS in its discussion of RBPA-12(iv) compliance. We recommend that DHS explicitly add the I-9 employment eligibility verification process to Option 1 ("Collecting Information To Conduct Direct Vetting") or Option 2 ("Use of Vetting Conducted Under Other DHS Programs."). This could be accomplished by leveraging the database developed pursuant to the USCIS I-9 program and selectively using it to vet personnel against the TSDB as needed.[17]

Increasing the functionality of Option 2 to the maximum extent possible is critical to implementing RBPS-12 in a way that is not overly burdensome. In order to minimize the compliance burden of the CFATS personnel surety requirements through reciprocity with other DHS background check programs, ISCD should follow its own guidance on RBPS-12 that states "… to minimize redundant background checks of workers, a person who has successfully undergone a security threat assessment conducted by DHS and is in possession of a valid DHS credential (such as a TWIC, hazardous materials endorsement (HME) license, NEXUS, or Free and Secure Trade (FAST) credential) will not need to undergo additional vetting by DHS. The facility, however, still must provide DHS with sufficient identifying information about the individual and his credential to allow DHS to verify that the credential still is valid."[18] However, in this ICR, ISCD has failed to follow its own guidance by not permitting reciprocity with these well-established vetting and credentialing programs *operated by DHS* without adding burdensome additional requirements – including the requirement that before such credentials can be used to satisfy RSPS 12, the facility must re-register with DHS each person having such a credential.

As a precondition to using these other credentials to satisfy RSPS 12, the facility must register each person leveraging such a credential through the PSP portal at least 48 hours in advance of unescorted access and must enter information about the DHS credential to be used so that ISCD can verify its validity, or in the case of individuals holding TWIC credentials, the facility must be equipped with a "reader".[19] Such preconditions fail to provide true reciprocity with these other programs. Holders of such DHS-issued security credentials have already been vetted by the federal government to each of the required RSPS 12 background check screens – identity, criminal history, citizenship, and terrorist ties. Although the PSP adds nothing to the rigor of the government's background check standards, ISCD puts itself forward as an arbiter of whether other DHS vetting and credentialing schemes are sufficient. This clearly defeats the purpose of reciprocity, and also fails to comport with DHS's professed goal stated in its own Guidance to "minimize redundant background checks of workers."[20] Moreover, this is not consistent with the role envisioned by Congress for ISCD or the CFATS program. ISCD's role should be to offer facilities a means to check against the TSDB those employees and unescorted visitors who have not been otherwise vetted against the TSDB by another equivalent federal background check program.

---

[17] DHS might believe that the statutory authorities under which USCIS collects data via the I-9 form do not extend to antiterrorism efforts. If this is in fact DHS's position, it should be able to segregate the data usage for employment eligibility from that of vetting against the TSDB to obviate any concerns about extending I-9 use for this purpose.

[18] RBPS Guidance Document at p. 97.

[19] We do note that coatings operations do not typically have employees who work within their covered facilities who have TWIC credentials, nor is it likely that they will obtain them.

[20] RBPS Guidance Document at 97, fn. 22.

Conclusion

In this ICR, DHS fails to implement RBPS-12 in a manner fully consistent with performance-based compliance systems. Rather, it does so in an unnecessarily burdensome and prescriptive way that fails to accommodate reasonable business practices. Nor does ISCD fully leverage parallel and potentially redundant DHS programs. The ICR also minimizes the difficulties that might be experienced by a facility seeking to comply with these requirements while also dealing with the practical requirements of running a chemical plant. In particular, the ICR fails to provide adequate justification for DHS's failure to allow regulated entities the ability to use other pre-existing vetting programs in a manner that will reasonably achieve DHS's need to keep known or suspected terrorists at bay without also requiring facilities to do so in a way that undercuts the advantages of leveraging these other programs -- many of which are conducted not only by other federal agencies, but by other programs within DHS itself. The Obama administration, like others before it, has repeatedly adopted as its goal the elimination of redundant or inefficient programs, as wasteful for the government and regulated community alike. All federal agencies that require security-based background checks should actively look for opportunities to harmonize the requirements for these checks and should reciprocally-recognize equivalent programs. The ISCD should carefully tailor the implementation of its personnel surety program so that it does not unnecessarily burden individuals already covered and vetted under other equivalent programs and the facilities employing them or using their services.

Thank you for your consideration of ACA's comments. Please do not hesitate to contact me at airish@paint.org if you have any questions or need any additional information.

Sincerely,

/s/

H. Allen Irish, Esq.
Director, Industry Affairs

*** Submitted via Regulations.gov ***