

June 4, 2013

DHS/NPPD/IP/ISCD CFATS Program Manager  
U.S. Department of Homeland Security  
Mail Stop 0610  
Arlington, VA 20528-0610

Re: CFATS Information Collection Request 1670-NEW,  
Docket No. DHS-2012-0061

Dear Sir or Madam:

The Society of Chemical Manufacturers and Affiliates (SOCMA) is pleased to submit these comments on the most recent Information Collection Request (ICR) published by DHS in support of its planned Personnel Surety Program (PSP) under the Chemical Facility Anti-Terrorism Standards (CFATS).<sup>1</sup>

For 91 years, SOCMA has been and continues to be the leading trade association representing the specialty chemical industry. SOCMA's 200 member companies employ more than 100,000 workers across the country and produce some 50,000 products – valued at \$60 billion annually – that make our standard of living possible. From pharmaceuticals to cosmetics, soaps to plastics and all manner of industrial and construction products, SOCMA members make materials that save lives, make our food supply safe and abundant, and enable the manufacture of literally thousands of other products. Over 80% of SOCMA's active members are small businesses.

Maintaining the security of our facilities has always been a priority for SOCMA members, and was so before September 11, 2001. After the tragic events of 9/11, SOCMA members did not wait for new government regulations before researching, investing in and implementing additional and far-reaching facility security measures to address these new threats. Under SOCMA's ChemStewards® initiative, SOCMA members were required to conduct security vulnerability assessments (SVAs) and to implement security measures. Many SOCMA member facilities have since become subject to the CFATS program and have implemented site security plans in conformance with it. These facilities are now in the process of being inspected and approved by DHS.

SOCMA backed enactment of the CFATS statute and has actively supported DHS in its implementation of the program, both in its individual capacity and through the Chemical Sector Coordinating Council (CSCC). We have been engaged throughout the development of the PSP, participating in CSCC's proposal to DHS in early 2011 and in

---

<sup>1</sup> 78 Fed. Reg. 17680 (Mar. 22, 2013).

comments filed by the CSCC or most of its members in response to prior ICRs in May 2010 and July 2011.

As explained more fully below—

- The current ICR announces several improvements to the PSP, which SOCMA appreciates. We particularly support:
  - Limitation of the PSP for now to Tiers 1 and 2; and
  - Authorization of innovative alternatives such as video monitoring.
- SOCMA reiterates its support of other important features of the PSP, primarily relating to the submission process, which DHS had previously announced and should retain.
- DHS has yet to address, much less justify, the additional burden required by a 48-hour prior notice requirement.
- We continue to question DHS's legal authority – at least without rulemaking – to require additional terrorist screening of individuals possessing a Transportation Worker Identification Credential (TWIC) or similar federal credential.

#### **I. SOCMA Supports Two New Features of the PSP**

SOCMA appreciates that DHS conducted significant outreach to the chemical sector in the past two years on the subject of personnel surety. The current ICR announces several new PSP approaches or details that are important improvements over the program as previously described, and SOCMA supports two of these in particular:

- **Limiting the PSP to Tiers 1 and 2.** DHS is clear that the PSP, as described here, would only be required for Tier 1 and 2 facilities, and that DHS would publish another ICR before applying it to facilities in Tiers 3 and 4.<sup>2</sup> This is a substantial improvement and SOCMA fully supports it, as most affected SOCMA member facilities are in Tiers 3 and 4. As DHS notes, this approach would allow it to evaluate the implementation of the PSP at riskier facilities, and see what lessons can be learned from the experience, before the burdens of the PSP are imposed on lower-risk facilities. This approach is also consistent with the risk- and market-based structure of the rule, as it will create a further incentive for facilities in Tiers 1 and 2 to voluntarily reduce the risks presented by their facilities so that they can move to Tiers 3 or 4.
- **Allowing “innovative escorting alternatives such as video monitoring.”**<sup>3</sup> Smaller facilities are especially unlikely to have free employees available to escort uncleared visitors. The ability to use existing, centralized or stationary security personnel to provide “virtual escorting” would make the PSP far less disruptive for many facilities.

---

<sup>2</sup> 78 Fed. Reg. 17696.

<sup>3</sup> *Id.* at 17682.

## II. SOCMA Supports Several Other Important PSP Features that DHS Should Retain

The workability of the PSP will depend crucially on a series of features that DHS has announced in prior ICRs, many in response to suggestions made by the CSCC. DHS should retain them.

### A. Beneficial Submission Features

SOCMA particularly supports the following features of the PSP submission mechanism:

- **Allowing third parties to submit information regarding prospective facility contractors and visitors.**<sup>4</sup> This includes both (i) companies like UPS submitting for their own employees and (ii) entities like safety councils simply serving an aggregating function and submitting on behalf of multiple facilities. The PSP simply will not work without this capability.
- **Not requiring facilities to audit such third parties.** The current ICR says: “The Department expects . . . that high-risk chemical facilities *could* audit and/or review their third party designees’ information collection and submission processes, to ensure that their designees submit appropriate information.”<sup>5</sup> CFATS facilities do not want terrorists getting access to their plants or systems. They also clearly understand that they retain the legal liability for compliance with RBPS #12 regarding contractors or other visitors for whom a third party has submitted information to DHS under PSP. But DHS is right to leave facilities with the flexibility to use their own business judgment regarding whether and to what extent they need to audit or otherwise review those third parties. A small facility may well conclude that it can trust a vendor like Federal Express or a large national tank truck company to comply effectively with a contractual commitment that the vendor makes to submit information on its employees to DHS for PSP purposes. The facility might also rely on a membership or cooperative organization to which it belongs to provide that sort of auditing, as many companies do now to audit the environmental compliance and stewardship of hazardous waste treatment, storage and disposal facilities. (Vendors might also appreciate being audited periodically by a representative entity, rather than over and over by every single CFATS customer they have.) At bottom, this is an issue of risk management and companies should be permitted to make their own judgments here, recognizing again that they retain ultimate legal responsibility.
- **Allowing consolidated corporate submissions that cover multiple CFATS facilities within that corporation.**<sup>6</sup> Many companies are sure to take this

---

<sup>4</sup> *Id.* at 17683.

<sup>5</sup> *Id.* at 17684 (emphasis added).

<sup>6</sup> *Id.*

approach. In many companies, relevant personnel are actually located at corporate headquarters rather than at facilities – this is particularly true in the case of cybersecurity. It would be wasteful for each facility to have to submit duplicative submissions for such individuals.

The current ICR does not repeat DHS’s earlier statement that **facilities would be free to determine which of their contractors (or categories of contractors) are considered “facility personnel” and which would be considered “visitors”** (and thus eligible for being escorted as an alternative to being pulled into the PSP process), “based on facility security, operational requirements, and business practices.”<sup>7</sup> This is an important and sensible way of making PSP more flexible, and DHS should reiterate it in the upcoming 30-day notice.

B. Other PSP Features that Should Be Retained

SOCMA also supports these PSP features:

- **The exclusions for (i) federal officials discharging their official duties, (ii) state and local law enforcement officials, and (iii) state and local emergency responders during emergency response situations.**<sup>8</sup> Federal employees will have been adequately screened in the normal course of their employment. State and local law enforcement personnel will also have been screened, and in any event, the balance of harms supports allowing them immediate access to sites even if they have not been. The balance tips even more dramatically toward immediate access for emergency personnel.
- **Allowing facilities to propose options not discussed in any ICR.**<sup>9</sup> No one can foresee now the myriad types of circumstances that will arise in which CFATS facilities will want to provide facility personnel and unescorted visitors with access to restricted areas and critical assets, or how facilities may propose to address screening such individuals for terrorist ties. The ICR wisely leaves room for facilities to propose options not yet foreseen.
- **Leaving blank fields in the submission format for companies to add their own identifying data.**<sup>10</sup> This is very helpful for allowing correlation between CFATs submissions and companies’ own human resources or other management information systems.

---

<sup>7</sup> See 76 Fed. Reg. 34721 n.1, 34727.

<sup>8</sup> 78 Fed. Reg. 17683.

<sup>9</sup> *Id.* at 17681.

<sup>10</sup> *Id.* at 17686.

### **III. Requiring 48-Hour Prior Notice Is Unduly Burdensome**

In its 2011 ICR, DHS mentioned for the first time that it was “considering” a requirement that CFATS facilities submit required PSP information for a new affected individual “at least 48 hours prior to access to restricted areas or critical assets.”<sup>11</sup> The current ICR never discusses the issue in text, but Table 3 (“Compliance Schedule for Option 1 and Option 2 . . .”) makes clear that this is now DHS’s intent.

The comments of most CSCC members in 2011 expressed concern about the disruption and costs that could be caused by a prior notice requirement. Neither the current ICR nor the Department’s March 11 letter responds expressly to these comments, so SOCMA repeats them here.

Chemical facilities frequently have important contractors and visitors arriving upon short or no notice. Such people may have to come on site unexpectedly – for example, if a production unit goes down or otherwise requires emergency maintenance. A requirement that the facility know the identity of the particular individuals who will or may be arriving at the plant in advance would impose a substantial burden. In order to maintain maximum flexibility, facilities would need to clear all such individuals as it anticipates might conceivably need to come on site – likely many more than might actually show up. For example, all technicians working for an electrical contractor, or all truck drivers working for a delivery truck company, might need to be identified, in coordination with those employers, and then their information submitted. This process would have to be repeated regularly to capture new hires, and yet would inevitably miss the most recent hires.

Facilities would also likely suffer collateral or indirect effects from not being able to clear someone as quickly as he or she is needed. Conceivably, a production unit might have to be shut down because it could not be repaired before the requisite minimum prior notice period expired. These effects could be severe – and could put facilities in a position of either violating CFATS or suffering significant losses. Clearly such serious consequences are a “burden” on facilities, and one that arises solely from the 48-hour prior notice requirement of this information collection. Yet the current ICR does not discuss them.

DHS may contend that the effects on plants of contractors or visitors being unavailable within 48 hours is somehow “indirect” and thus not cognizable under the Paperwork Reduction Act. Still, the considerable effort that companies will have to expend repeatedly in order to clear every possible employee of a business that they might need on short notice does fall within the traditional conception of “paperwork” burden, as it is

---

<sup>11</sup> 76 Fed. Reg. 34724.

the cost of “developing . . . and utilizing . . . systems for the purpose of collecting . . . information.”<sup>12</sup>

DHS could eliminate these burdens by allowing facilities to submit information on new affected individuals at the time those individuals require access to a restricted area or critical asset.

The current ICR does make reference to “emergency or exigent situations” that may require “access to restricted areas or critical assets by . . . individuals who have not had appropriate background checks[; f]or example, emergency responders” in (evidently) non-emergency situations.<sup>13</sup> The ICR says:

If high-risk chemical facilities anticipate that any individuals will require access to restricted areas or critical assets without visitor escorts or without the background checks listed in RBPS 12 under exceptional circumstances, facilities may describe such situations and the types of individuals who might require access in those situations in their SSPs or ASPs. The Department will assess the appropriateness of such situations, and any security measures to mitigate the inherent vulnerability in such situations, on a case-by-case basis as it reviews each high-risk chemical facility's SSP or ASP.<sup>14</sup>

This approach may help ameliorate the 48-hour prior notice requirement. It would be helpful if DHS would clarify the “situations” to which it is referring, so it would be clear that these encompass equipment breakdowns and similar circumstances that—

- Are unforeseeable (or at least where, even if the kind of event is foreseeable, whether and when it might occur is unpredictable<sup>15</sup>); and
- Require the physical presence of specific types of personnel whose particular identities at a given time cannot be predicted with any degree of assurance.

It would also help if DHS were to state that such circumstances are likely to arise for all or most facilities at some point, and hence site security plans that provide for them would be approvable so long as they are reasonably specific about—

- The facility’s potential needs (i.e., the kinds of circumstances where nonemployees might be needed in fewer than 48 hours); and
- How the facility would address personnel surety in such cases (i.e., when and why it might be unreasonable or infeasible to escort contractors or visitors).

---

<sup>12</sup> 5 C.F.R. § 1320.3(b)(1)(ii).

<sup>13</sup> 78 Fed. Reg. 17683.

<sup>14</sup> *Id.*

<sup>15</sup> This would be comparable to a plant getting fire insurance – because fires are foreseeable, even if whether and when one might have a fire is unpredictable.

#### **IV. Facilities Should Be Able To Accept TWICs and Similar Credentials Without Further Screening. DHS Needs To Conduct Rulemaking To Require More**

In their July 2011 comments, CSCC members explained why the current CFATs rule does not authorize DHS to require facilities to go beyond accepting TWICs and similar credentials from individuals possessing them. The Department's March 11, 2013 letter<sup>16</sup> does not address the merits of these arguments. For convenience, we repeat them here.

The statutory authority under which DHS has issued the CFATS rules is a rider to an appropriations statute and is quite general – it provides merely that DHS “shall issue interim final regulations establishing risk-based performance standards for security of chemical facilities.”<sup>17</sup> Importantly, however, it leaves the choice of security measures to the facility, so long as they satisfy the relevant standard:

[S]uch regulations shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility[; and] the Secretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section.<sup>18</sup>

Thus, DHS has statutory authority only to require attainment of the performance standard that it sets, not to prescribe how a facility achieves attainment. Put another way, DHS must accept any security measure that meets the applicable performance standard.

The performance standard driving the PSP – RBPS #12 – is that regulated facilities “[p]erform 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 . . . [m]easures designed to identify people with terrorist ties.”<sup>19</sup>

This regulatory text does not itself mention the Terrorist Screening Database, or require facilities to submit any information to DHS. It certainly does not require facilities to give DHS information so that DHS can develop and maintain databases that keep track of which “affected individual[s] may be associated with [which] high-risk chemical

---

<sup>16</sup> Letter to Alexis Moch from David Wulf (March 11, 2013).

<sup>17</sup> Pub. L. No. 109-295, § 550(a), 6 U.S.C. § 121 note.

<sup>18</sup> *Id.*

<sup>19</sup> 6 C.F.R. § 27.230(a)(12).

facilities.”<sup>20</sup> The rule text only requires that facilities perform “appropriate” background checks and ensure “appropriate” credentials “to identify people with terrorist ties.”

DHS currently issues roughly a half-dozen credentials that require, as a condition of issuance, that DHS check the applicant against the TSDB – most notably including the Transportation Worker Identification Credential (TWIC) and the Hazardous Materials Endorsement (HME) to a commercial drivers license. Moreover, DHS recurrently vets these credentials against the TSDB so that it will discover if a holder subsequently is added to the TSDB – it describes this as “a DHS best practice.”<sup>21</sup>

A great many of the contractors and visitors that may require access to a CFATS-regulated facility possess one of these credentials. In our considered view, a facility has satisfied its obligation under RBPS #12 if it determines that an individual possesses one of them. We believe that any additional requirement for facilities to submit information regarding these individuals to DHS is beyond DHS’s ability to compel, especially since DHS already has the ability to vet these persons’ credentials on a continuing basis and, if it gets a hit against the TSDB, to revoke the credential, alert the FBI so that it can place the person under surveillance, etc. We do not believe DHS has the authority to enlist regulated facilities as part of its scheme to keep track of which people are associated with (i.e., have ever had access to the restricted areas of) a regulated facility, in the highly unlikely event that one of them will turn out, after having obtained a TWIC or similar credential, to have some terrorist tie.<sup>22</sup> In short, we not believe RBPS #12 currently empowers DHS to compel our members to facilitate a DHS best practice.

In its March 11 letter (at 2), DHS says that it needs facilities to supply additional data regarding individuals holding TWICs or similar credentials (i) so that it can verify that the individual is still enrolled in the relevant program and (ii) to enable DHS to access the individual’s original enrollment data and the results of prior TSDB vetting of that individual “when necessary.”

It is not obvious, however, that RBPS #12 requires facilities to enable DHS to do either of these things. RBPS is focused on what facilities must do, and requires them to “ensure appropriate credentials” and implement “measures designed to identify people with

---

<sup>20</sup> 78 Fed. Reg. 17684) (“The Department is aware that an affected individual may be associated with multiple high-risk chemical facilities, and thus information about an affected individual may be submitted to the Department multiple times by different high-risk chemical facilities . . .”).

<sup>21</sup> *Id.* at 17682 n. 7.

<sup>22</sup> In its March 11 letter (at 2), DHS says that it “will not track the movements of affected individuals . . . from chemical facility to chemical facility.” But, as the latest ICR continues to state, DHS will be “associat[ing] affected individual[s with the] different high-risk chemical facilities” to which those individuals have access. *See* note 20 *supra*.

terrorist ties.” Determining that a person has a valid TWIC or similar credential – a credential that would be cancelled if DHS thought a person had terrorist ties – accomplishes this. For DHS to verify the validity of the credential a single time – when a person first seeks access to a facility – adds very little to this. Indeed, if DHS wanted to guard against persons with cancelled TWIC cards continuing to use them, it should give facilities electronic access to the cancelled card list. DHS has not explained why it could not do so. DHS has also not explained why it would be “necessary” for DHS to access a person’s original enrollment data or the results of prior vetting.

The March 11 letter adds (at 2) that facilities now have the option of using TWIC readers to validate the TWICs of persons carrying them, and could avoid submitting information regarding these individuals to DHS. As DHS is aware, the Government Accountability Office recently issued harsh criticism of TSA’s TWIC reader pilot program, concluding that, “[e]ven years after initiation, DHS has not demonstrated how, if at all, TWIC will improve maritime security.”<sup>23</sup> In light of this finding, it may well be difficult for security personnel at facilities to obtain approval to buy readers – and so this option is not as helpful as it might appear.

Finally, the March 11 letter asserts (at 2) that making facilities gather and submit additional information for individuals possessing a TWIC or similar credential “will not be beyond the scope of the Department’s statutory or regulatory authority.” But it does not explain why that is so, or how the foregoing arguments are wrong. If DHS believes it has the statutory authority to mandate as specific a performance measure as the PSP, it needs to go through rulemaking to seek to amend its CFATS performance standards to specifically require that action.

Thus – at least with respect to individuals who possess credentials like the TWIC or HME – the PSP continues to be not “necessary for the proper performance of the functions of the agency,” and cannot be approved under the PRA.<sup>24</sup> Similarly, for those individuals, the PSP’s requirement that such facilities collect and submit to DHS information about their credential serial numbers, expiration dates, and (in the case of HMEs) issuing state is “unnecessarily duplicative of information otherwise reasonably

---

<sup>23</sup> GAO, GAO-13-198, TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL: CARD READER PILOT RESULTS ARE UNRELIABLE; SECURITY BENEFITS NEED TO BE REASSESSED (May 2013), “What GAO Found.”

<sup>24</sup> See 44 U.S.C. § 3508 (“Before approving a proposed collection of information, the Director shall determine whether the collection of information by the agency is necessary for the proper performance of the functions of the agency . . .”). Cf. OMB, THE PAPERWORK REDUCTION ACT OF 1995: IMPLEMENTING GUIDANCE 38 (Preliminary draft Feb. 3, 1997) (“The term ‘need’ means that some programmatic or policy requirement (as opposed to a desire for information . . .) exists.”).

accessible to the agency.”<sup>25</sup> For this reason as well, OMB should disapprove the ICR if DHS does not correct it by the date of the 30-day notice.

\* \* \*

SOCMA appreciates the opportunity to submit these comments. If you have any questions concerning them or would like clarification of any, please do not hesitate to contact me at 202-721-4122 or [allmondb@socma.com](mailto:allmondb@socma.com).

Sincerely,

A handwritten signature in black ink that reads "WE Allmond". The signature is written in a cursive, slightly stylized font.

William E. Allmond IV  
Vice President of Government & Public  
Relations

---

<sup>25</sup> 44 U.S.C. § 3506(c)(3)(B); *cf.* PAPERWORK REDUCTION ACT GUIDANCE, *supra*, at 40 (“The term ‘unnecessary duplication’ means that information similar to or corresponding to information that could serve the agency’s purpose and need is already accessible to the agency.”).