U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

May 21, 2013

David M. Wulf
Director
Infrastructure Security Compliance Division
Office of Infrastructure Protection
U.S. Department of Homeland Security
Washington, D.C. 20528

Re: Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program (PSP), Docket No. DHS-2012-0061

Dear Mr. Wulf:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, sector, and region, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, welcomes the opportunity to comment on the U.S. Department of Homeland Security's (DHS's) information collection request related to the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program (PSP).[1]

The Chamber appreciates that DHS withdrew its PSP proposal from the Office of Management and Budget last year. It is a positive development that the department has adopted some of industry's suggestions to help establish a smart and effective personnel surety framework. Still, more needs to be done to create a *flexible* program that is consistent with the base standard (RBPS 12–Personnel Surety)—which is intended to set the desired outcome but leaves the specific measures or techniques to achieve that outcome up to the discretion of the regulated entity.[2] Without a workable PSP, the department would be unable to approve a covered facility's security plan.

[1] See March 22, 2013, *Federal Register*, pp. 17680–17701, via www.gpo.gov/fdsys/pkg/FR-2013-03-22/pdf/2013-06184.pdf.

[2] See www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf, p. 96.

The Chamber, like DHS, wants a CFATS program that is managed well and enhances the safety and security of approximately 4,000 high-risk chemical facilities across America. We urge the department to adopt the following recommendations in the spirit of public-private collaboration:

First, among the changes to the PSP, it is constructive that DHS intends to limit initial implementation to tier 1 and tier 2 chemical facilities. The department also intends to allow covered facilities and third-party contractors to use the Transportation Worker Identification Credential (TWIC).[3] However, it would be useful for DHS to further clarify its thinking behind the PSP in relation to the facilities' need for transparency and strong personnel assurance.

CFATS requires that companies vet individuals' personal information against the Terrorist Screening Database (TSDB) before they are granted access to restricted areas or critical assets of a high-risk chemical facility. However, DHS does not automatically plan to notify facility owners and managers when there are positive matches against the TSDB. This approach seems contrary to CFATS' intent, which is to mitigate terrorist risks to facilities and nearby communities.

The Chamber believes that facilities should have the option of being notified when an individual is listed on the TSDB. (In a similar vein, the PSP needs to provide a means of allowing personnel to challenge indications that they are a security risk.) It seems reasonable that companies should have the right to be made aware of when individuals have been screened against the TSBD and cleared *before* they access facilities' sensitive areas.

Second, the prescribed nature of submitting data to the government cuts against the performance-based design of CFATS. Specifically, there is seemingly limited value in submitting information to DHS 48 hours in advance of individuals visiting a facility if the department is not going to notify owners and operators that personnel have been properly vetted and cleared prior to entry.

Third, DHS continues to underestimate the workload involved in compiling personnel information for submission to authorities. Federal programs like CFATS generally put the onus on individuals to submit their information to the government. In contrast, the PSP puts the weight of collecting and submitting data directly to DHS squarely on businesses.

---

[3] See http://csat-help.dhs.gov/pls/apex/wwv_flow_file_mgr.get_file?p_security_group_id=100060&p_fname=PersonnelSurety60DayICRFS_March2013.pdf, p. 2. Also, TWIC reader requirements (proposed rule) are under review by the Coast Guard (see www.gpo.gov/fdsys/pkg/FR-2013-05-10/pdf/2013-11227.pdf).

As a remedy, the Chamber believes that DHS should establish a secure online portal (optional) to enable individuals to submit their information directly to the department. Such an initiative would help reduce the burdens on the regulated facilities for collecting and keeping individuals' information, which could have unwanted privacy and legal implications. Also, the initiative would be consistent with the administration's insistence (e.g., in the context of cybersecurity legislation) that businesses take reasonable steps to remove personal information when sending data to the government.[4] An online portal would remove or substantially limit businesses' role in collecting and sending private information to federal officials.

The Chamber appreciates the opportunity to recommend ways to make the PSP more workable, effective, and consistent with a flexible risk-based security framework. If you have any questions or need further information, please do not hesitate to contact me (abeauchsene@uschamber.com; 202-463-3100) or my colleague Matthew Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne

[4] See www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf, p. 1.