



One Hundred Thirteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

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: *Department of Homeland Security Docket Number DHS-2012-0061*
Information Collection Request: Chemical Facility Anti-Terrorism Standards Personnel
Surety Program

Dear Sir or Madam:

As the U.S. Representative for the 2nd District of Mississippi, Ranking Member of the House Committee on Homeland Security, and an original author of Chemical Facility Anti-Terrorism Standards (CFATS) legislation, I submit the following comments to the Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Chemical Facility Anti-Terrorism Standards Personnel Surety Program, New Information Collection Request: 1670—NEW, Docket No. DHS-2012.0061.¹

COMMENTS

In general terms, I am pleased that the Department has engaged the private sector, through conference calls with industry associations and meetings with Chemical Sector Coordinating Council leadership and members, and believe that these efforts have positively impacted this Information Collection Request (ICR). Certainly, allowing an owner or operator of a facility to do “one time” submissions of Personally Identifiable Information (PII) for permanent or extended assignment employees, permitting third-party submissions, and allowing company-wide submissions for regulated companies with multiple facilities are improvements.

However, I continue to have concerns with the Personnel Surety Program (PSP), as developed to meet the requirements of Risk-Based Performance Standard (RBPS) 12. Of the 18 CFATS Risk-Based Performance Standards, RBPS 12 is the only one that

¹ <http://www.gpo.gov/fdsys/pkg/FR-2013-03-22/html/2013-06184.htm>

necessitates government assistance; a high-risk chemical facility is required to vet an individual seeking unescorted access to that facility against the Terrorist Screening Data-Base (TSDB) to ascertain whether the individual has terrorist ties.²

The Department has acknowledged that performance standards specify the outcome required but leave the specific measures to achieve that outcome up to the discretion of the regulated entity.³ That seems to be the Department's view with respect to all the Risk-Based Performance Standards, except for RBPS 12. To comply with RBPS 12, the Department would require a facility owner or operator to: (1) at least 48 hours before the facility grants unescorted access to a person, submit information to the Department for vetting or (2) validate a Transportation Worker Identification Credential (TWIC) through a biometric reader.

While I am pleased that the ICR seeks to provide an option to a facility owner or operator who would like to manage personnel surety on-site, without having to aggregate and send personally identifiable information of their staff, contractors, and visitors to the Department, I have some reservations about plans to integrate TWIC into PSP. Specifically, the PSP would allow a facility to electronically verify and validate an individual's TWIC through the use of a TWIC reader. Unfortunately, the TWIC program is not fully implemented. Furthermore, the future of an essential regulation setting forth how biometric readers could be used to validate TWICs is in question, in light of a recent Government Accountability Office (GAO) review. On May 8, 2013, GAO reported that the pilots undertaken by the Transportation Security Administration to test the use of biometric cards and readers in the maritime environment had produced results that were 'incomplete, inaccurate, and unreliable.'⁴ GAO recommended that the DHS suspend efforts to finalize pending TWIC regulations until the successful completion of a security assessment of the effectiveness of using TWIC.

I have concerns about the accuracy of estimates of the administrative burden of the PSP and the number of individuals that would be subject to this vetting. I also have concerns about the extent to which this ICR has considered recognizing other TSDB-vetted credentials.

Additionally, I have questions about the appropriateness and achievability of the 48-hour requirement. In particular, I am not convinced about the value of this submission from a security standpoint, since the Department has said that after receiving this information

² RBPS 12: "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[.]"

³ "Risk-Based Performance Standards Guidelines: Chemical Facility Anti-Terrorism Standards," DEPARTMENT OF HOMELAND SECURITY, May 2009 at p. 10.

⁴ <http://www.gao.gov/products/GAO-13-198>

from a facility, it does not necessarily intend to notify the facility whether the person vetted presents a terrorist risk and thereby should be precluded from access to the facility, let alone unescorted access. I would urge the Department to assess the security value of the 48-hour requirement and its position that notifications will not be furnished to facility owners and operators.

If the Department contends that the 48-hour requirement for vetting and validation should stand, I would urge the Department to make available a wider range of options for compliance, including the submission of other existing TSDB-based credential programs that could be effectively cross-referenced to facilitate PSP, such as the Hazardous Materials Endorsement Program, the Trusted Traveler programs including NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Free and Secure Trade (FAST), or Global Entry. Additionally, the Department should establish a secure web portal as another avenue for submission where an individuals seeking unescorted access to submit their personally identifiable information and receive a unique identifier that could be presented to the facility owner or operator to gain access. This approach makes sense from a privacy perspective, particularly for contractors and other individuals who seek unescorted access to a CFATS-regulated facility but are not employed by that facility.

Thank you for the opportunity to file these comments. Should you have any questions or concerns, please contact Rosaline Cohen, Chief Counsel for Legislation for the Committee on Homeland Security, at (202) 226-2616.

Sincerely,


Bennie G. Thompson
Ranking Member