IME
institute of makers of explosives

The safety and security institute of the commercial explosives industry since 1913

July 15, 2013

TSA PRA Officer
Office of Information Technology
Transportation Security Administration
US Department of Homeland Security
Washington, DC 20528

VIA Email: TSAPRA@dhs.gov

RE: TSA-2006-24191[1]
Information Collection Request: Transportation Worker Identification Credential Program

Dear Sir or Madam:

On behalf of the Institute of Makers of Explosives (IME), I am submitting comments on the U.S. Department of Homeland Security's (DHS) Transportation Security Administration (TSA) information collection request (ICR) to extend the approval of its revised application form for used by those seeking a Transportation Worker Identification Credential (TWIC).

Interest of the IME

IME is a nonprofit association founded in 1913 to provide accurate information and comprehensive recommendations concerning the safety and security of commercial explosive materials. IME represents U.S. manufacturers and distributors of commercial explosive materials and oxidizers as well as other companies that provide related services. The majority of IME members are "small businesses" as determined by the U.S. Small Business Administration.

Millions of specialty explosive devices are manufactured annually in the United States for domestic and worldwide commerce. These devices are essential to metals and minerals mining, oil and natural gas production, and construction industries. The ability to manufacture, use, transport and distribute commercial explosives safely and securely is critical to the Nation's economic well-being and the quality of life we enjoy.

Explosive products and precursors are transported by all modes. The transportation of these materials is closely regulated to ensure the safety and security of these shipments. We credit adherence to these requirements and industry best practice standards for the exceptional safety record and low theft/loss rates of products we transport.

[1] 78 FR 32417 (May 30, 2013).

Background

Background vetting of individuals is among the most common practices used to secure assets or activities against criminal and terrorist threats. Since 2003, all employees who may possess explosives, whether possession is actual or constructive, have been subject to vetting by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The ATF vetting standard requires: verification of identity; a check of criminal history to a specified list of crimes; verification of legal authorization to work; and a determination that the individual has no terrorist ties. Subsequently, ATF's requirements became the basis for vetting standards in threat assessments used by TSA under the agency's Transportation Worker Identification Credential (TWIC), Hazardous Materials Endorsement (HME), Free and Secure Trade (FAST) card, and Secure Identification Display Area (SIDA) badge programs. By using standards equivalent to ATF's requirements, TSA triggered the exception for transportation workers from the Bureau's vetting requirements found in Federal Explosives Law. At the same time, IME members find themselves regulated by other DHS programs that will cause their employees to again be subject to multiple vetting programs. It is with this perspective that we offer the following comments.

Comments

- Avoiding Regulatory Overlaps: A purpose of the Paperwork Reduction Act is to "minimize the burden of the collection of information on those who are to respond." OMB accomplishes this information minimization task through the ICR process. Redundancy between threat assessment programs wastes public and private resources without offsetting security benefits. IME has long-recognized and advocated for equivalent security vetting standards to be used by the federal government to assess the threat presented by individuals with access to restricted assets or critical infrastructure. Our goal eventually is to consolidate the myriad vetting programs and move to one common access credential or clearance to engage in security-sensitive activities. Ostensibly, this outcome was the genesis of the TWIC program.

  Short of this goal, equivalent standards open the door for reciprocal recognition of various program credentials and clearances that share those standards. Among the directives issued by the White House as part of it assessment of surface transportation security is one that agencies should implement the principle of "enroll once, use many," meaning that the government should reuse threat assessment information it already has on individuals who are applying for multiple access privileges. ATF's recognition of TSA transportation worker threat assessments is a step in this direction, and TSA has made efforts to ease the redundancy between the TWIC and the HME. But, the only TSA program that currently grants full reciprocity among equivalent vetting programs is that for air cargo security. The reciprocal approach taken under the Air Cargo program has proven successful. It should be a model for other federal vetting programs to follow.

  Regrettably, instead of following an approach like that of the Air Cargo program, DHS' Infrastructure Security Compliance Division (ISCD) is attempting to implement two new stand-alone vetting programs – one under the Chemical Facility Anti-Terrorism Standards (CFATS) program and one under the Ammonium Nitrate Security Program (ANSP) – which would require vetting of individuals who have already been cleared through the ATF or one of the TSA threat

assessment programs. ISCD's determination to establish separate redundant vetting programs is even more unsustainable given the fact ISCD has asked TSA to perform the vetting. As of December 31, 2012, ISCD had paid TSA $7.7 million as a placeholder for its yet-to-be-launched CFATS' Personnel Surety Program (PSP) although not one name has been vetted. More disturbing, in this time of constrained federal resources, is the fact that ISCD rejected an offer from the U.S. Department of Justice's Terrorism Screening Center (TSC) to conduct terrorist ties vetting at "no cost".[2] The TSC performs the ATF threat assessments, and TSA uses a "mirror image" of the TSC data to perform its vetting. IME has taken every available opportunity to inform the Department and OMB that failure of ISCD and TSA to grant full reciprocity, without preconditions, between equivalent federal vetting programs is an unwarranted burden on industry and a waste of scarce federal resources.

The TWIC application form TSA is submitting to be authorized under this ICR opens the door to leveraging, without preconditions, the TWIC as an option to address the problem of subjecting individuals to multiple threat assessment programs. (See attached.) The form has been modified in Section 1, Part A, to allow individuals, other than transportation workers, to apply for a TWIC. This application modification gives TSA an easy path to implement the authority the Secretary has to determine that other categories of individuals are eligible to obtain TWICs.[3] We fully support this modification.

The form modification does not displace the Secretary's discretionary authority to determine which categories of individuals may be allowed to apply for the TWIC. Additional categories of individuals would have to be "authorized by TSA." We have asked TSA to establish and publish the process by which categories of individuals could petition TSA to be authorized to apply for TWICs. We are anxious to put in place a process to request TSA authorization so that we can petition the agency to allow those required to obtain a threat assessment under the new vetting programs of ISCD an alternative means of compliance. While TSA has been open to working with us on this request, the agency has expressed reluctance to allow non-transportation groups to apply for TWICs. TSA's reticence is founded in the belief that federal law precludes the agency from assessing fees for TWICs from non-transportation applicants. This is not the case. While federal law requires TSA to collect TWIC application fees from those "in the field of transportation," it does not preclude the agency from collecting the same fees from all who apply for a TWIC.[4] [5]

We understand that TSA plans to launch this new form in August. We hope that OMB will quickly approve the form, and that TSA will finalize a process to request authorization to use the form before ISCD finalizes its PSP.

---

[2] Effectiveness of the Infrastructure Security Compliance Division's Management Practices to Implement the Chemical Facility Anti-Terrorism Standards Program, OIG-13-55, March 25, 2013, (hereinafter *DHS-OIG Report*), page 29-30, http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-55_Mar13.pdf.

[3] 46 U.S.C. 70510(b)(2)(G).

[4] 6 U.S.C. 469.

[5] During the June 18, 2013 House Subcommittee on Border and Maritime Security hearing, "Threat, Risk and Vulnerability: The Future of the TWIC Program," it was pointed out that Rep. Sheila Jackson Lee's TWIC was due to expire shortly. Rep. Jackson Lee is not a "transportation worker". She no doubt paid fees to obtain her TWIC.

- Employer notification: The Paperwork Reduction Act also asked agencies to "evaluate … whether the information will have practical utility." A security gap is created by ISCD under the proposed PSP because the agency "will not routinely notify high-risk chemical facilities of Personnel Surety Program vetting results" irrespective of which vetting option is used through the PSP portal. This policy is inconsistent with other federal security vetting programs used by the private sector. Without notice of the results of vetting, facilities are unable to affirm that individuals with access to restricted areas do not present a security threat. Facilities will not be able to stop those with "terrorist ties" from entering, accessing and/or controlling critical infrastructure assets. As such, the PSP provides facilities no security value. This security gap is closed under the TWIC program. Facilities that accept this credential know that the individual possessing it has been determined not to present a terrorist risk. TSA "perpetually" vets the identities of TWIC holders against the TSDB. Under the TWIC program, TSA provides facilities access to a "cancelled card list" based on this perpetual vetting practice and has proposed rules to implement electronic card readers that allow facilities to determine in near real time the status of a holder's threat assessment. This information collection has "practical utility."

- GAO Evaluations: GAO has undertaken a number of reviews of the TWIC program since its inception. These reports seem to be ever more critical of the TWIC program. The most recent report, released earlier this year, goes so far as to recommend that Congress "halt" promulgation of a final regulation until the successful completion of a security assessment of the effectiveness of using TWIC, and that the assessment include consideration of an alternative "decentralized and locally managed approach" to personnel vetting.[6] We are very concerned about the tone and direction advocated by the GAO. While the TWIC program and its value to the public can be enhanced as noted above, it affords a level of security vetting and identity verification that has never before been possible. The TWIC provides a uniform, industry-wide, biometric, tamper-resistant credential that is not matched by any other security vetting program offered to the public. Even the U.S. Department of Defense has recognized the TWIC as equivalent to its CAC (common access card). No other security credential issued to the public has that standing.

  The critics of the TWIC would do well to remember that security vetting is one aspect of access control. While the TWIC can be used to authorize access, possession of the credential does not, in and of itself, grant the holder a "free pass" to access any secure area. The primary purpose of the TWIC is to establish the identity of the credential holder, and confirm that that individual does not pose a terrorist threat. It is the facility owner/operator that ultimately controls access to secure areas through its approved security plan and procedures.

- OMB Recommendations: TSA submitted an emergency ICR last year to account for the reduced hours anticipated to result from the agency's decision to issue 3-year extensions of TWICs that are coming due at a reduced cost to holders inasmuch as the TWIC reader rule is still pending. Additionally, OMB expressed concern about the low response rate TSA obtained for users to support the burden estimate. OMB recommended that TSA consider offering the survey in Spanish as a way to boost the sample size of respondents. While IME is not taking a position on the merits of language options for the survey, we do affirm on behalf of our members the value

[6] http://www.gao.gov/assets/660/654431.pdf.

of this program to assess the security threat of individuals with needs for unescorted access to security-sensitive assets or activities, and we fully support TSA's decision to offer holders an option to extend the expiration date of expiring credentials for three years.

Conclusion

Millions of workers are currently subject to some kind of federal security vetting program. The federal government has adopted a four-part standard that has been adopted in a variety of venues as sufficient to determine that individuals seeking access privileges to restricted areas and activities do not present a security threat. By adopting policies where credentials and clearances can be reused, as is the case with the Air Cargo program, these workers are spared from having to comply with burdensome, redundant and costly vetting procedures which provide no commensurate security benefit. The TWIC program was envisioned to be the single security vetting program for transportation workers, and with the modifications included in this version of the application form, has the potential to be the security vetting program of choice for any number of categories of individuals for which a threat assessment is required. This application form modification should be supported.

Thank you for the opportunity to comment.

Respectfully,

Cynthia Hilton

Cynthia Hilton
Executive Vice President

Attachment