

IME
institute of makers of explosives
SECURITY VETTING & CREDENTIALING REFORM

Issue: Should federal security vetting and credentialing of employees be reformed?

Background: The purpose of federal security vetting and credentialing programs is to ensure that security-sensitive workers do not pose a threat to national security. DHS currently operates seven background check programs covering security-sensitive work environments – HME, TWIC, FAST, SIDA, PSP, Air Cargo and IAC. More – LASP and AN Security– have been proposed.¹ DOD, ATF and NRC operate other employee vetting programs. Often the populations covered by these vetting programs overlap. States are also allowed to impose their version of security checks on these populations. Commercial drivers, more than any other class of worker, encounter circumstances where they may be required to submit to more than one security check. Affected stakeholders have worked to fix a number of flaws arising from the multiplicity of background check programs. Improvements have been made to promote reciprocity between TWIC and HME, and between PSP and other federal vetting program. Still, issues remain.

Concerns: Virtually all individuals subject to federal worker vetting and credentialing programs are successfully screened. The redundancy of programs is costly to the government and covered individuals and, since core disqualifications are the same, there is no value added. Aspects of some programs have reached beyond rooting out terrorists seeking access to critical assets or materials. While DHS has harmonized disqualifications, only the IAC and CFATS-PSP provide full reciprocal recognition of other DHS background credentials – the latter required congressional action (P.L. 113-254). State-allowed differences include background data to be collected; standards for disqualification, appeal and rehabilitation; and fees. Finally, only under the HME and ATF programs are employers provided information about the disposition of their employees’ background checks. Without such information, employers are unable to prevent individuals identified as security threats from transporting hazardous materials, rendering the background check ineffective and undermining employer efforts to protect the public and their other employees.

The administration has begun to address some of these concerns. TSA has issued an encompassing interpretation of who is “in the field of transportation” and therefore eligible to apply for a TWIC. TSA has also acted to reuse Personally Identifiable Information (PII) submitted under the TWIC and HME for other programs like TSA Pre✓[®]. Senator John Thune (R-SD) introduced legislation in the 115th Congress, S. 763, to advance these goals. These initiatives should be supported.

Recommendations: To address these matters, IME recommends that –

- Security threat disqualifications should be reviewed and harmonized across all federal vetting programs.

¹ **Key Federal Programs:**

- HME Threat Assessment – PL 107-56 (USA Patriot Act)
- TWIC – PL 107-295 (MTSA)
- SIDA – PL 107-71 (ATSA)
- FAST – http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/fast/
- IAC (voluntary) – 49 USC 44920 (ATSA)
- LASP (proposed October 30, 2008)
- CFATS-PSP (ICR finalized December 18, 2015)
- ATF Explosives – PL 107-296 (HSA)
- NRC – 10 CFR 73 App. B
- DOD – MFTRP-1C-R 2nd edition
- AN Sec (NPRM proposed August 3, 2011)
- Trusted Traveler Programs (CBP)

- A single base credential should be developed for all those needing unescorted access privileges to restricted assets. The credential should, like the TWIC, establish identity, and should be recognized as a sufficient security credential for federal purposes.
- The credential should be portable.
- The scope of vetting and credentialing programs should be limited to apply only to those individuals with unescorted access to critical infrastructure and key resources.
- The confidentiality of the information obtained in the course of conducting the background records checks should be protected as sensitive-security information.
- Credential “readers” should not be required unless mandated by Congress.
- Non-federal entities should be prohibited from requiring separate security background checks or credentials for workers needing access to security-sensitive venues or activities.
- Program revisions should be determined by notice and comment rulemaking.
- Congress should enact legislation that supports these principles.