

December 2011

# TRANSPORTATION SECURITY

## Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload

U.S. Government Accountability Office

GAO90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

## Why GAO Did This Study

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) manages several credentialing programs, which include background checking (known as Security Threat Assessments) and issuing credentials to transportation workers requiring unescorted access to the nation's transportation facilities. The number of TSA programs and their potential for redundancy with state and local government programs has raised questions about these credentialing programs. In response to a mandate in the Coast Guard Authorization Act of 2010, GAO examined TSA credentialing programs to identify (1) the roles and responsibilities of federal and nonfederal government entities related to TSA's transportation worker credentialing programs and how they compare, and (2) any key challenges TSA faced in ensuring the effectiveness of its credentialing programs. GAO reviewed program documentation, such as program processes, and conducted structured interviews with selected airports, port authorities, and state agencies. GAO selected nonfederal government entities based on volume of passengers, truckers, and cargo.

## What GAO Recommends

GAO recommends that (1) TSA and the FBI conduct a joint risk assessment of TSA's access to criminal history records, (2) TSA assess costs and benefits of using state-provided criminal history information, and (3) TSA develop a workforce staffing plan to address its growing Adjudication Center workload.

DHS and DOJ concurred with GAO's recommendations.

[View GAO-12-60 or key components.](#)  
For more information, contact Stephen M. Lord at (202) 512-4379 or [lords@gao.gov](mailto:lords@gao.gov).

## TRANSPORTATION SECURITY

### **Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload**

## What GAO Found

Nonfederal government entities have varying roles and responsibilities under three TSA transportation worker credentialing programs we reviewed—the Transportation Worker Identification Credential program (TWIC) for maritime workers; the Hazardous Materials Endorsement program (HME) for truckers seeking a commercial drivers license endorsement to carry hazardous materials; and the Aviation Workers program for airport workers. TSA administers the TWIC credentialing process, with no role for maritime port facility operators outside of verifying issued credentials. Under HME, state licensing agencies issue endorsements based on whether TSA reports favorable background checking results. In contrast, under the Aviation Workers program, TSA and airports share responsibility for the vetting process for airport workers, with airports responsible for enrolling applicants, adjudicating criminal history results TSA provides, and issuing, and if necessary, revoking airport badges. Eleven of 17 selected maritime ports—including 4 of the top 10 largest ports—reported implementing additional credentialing requirements to those under TSA regulations, which generally included requirements for applicants to obtain and present local port identification—in addition to a TWIC—to gain unescorted access. At three of these ports, local agencies conducted additional criminal history checks. In addition, 4 of 6 selected state licensing agencies responsible for issuing commercial drivers licenses were conducting additional criminal history checks on HME applicants. Some programs included applicant fees which added to the costs already incurred by applicants in obtaining TSA credentials. However, port officials reported their programs provided additional benefits over TSA's programs. The state and local credentialing programs we reviewed complemented the existing credentialing programs administered by TSA.

TSA faces challenges in ensuring it has the necessary information and appropriate staffing to effectively conduct Security Threat Assessments for applicants to its transportation worker credentialing programs. First, in general, the level of access that TSA credentialing programs receive to Department of Justice (DOJ) Federal Bureau of Investigation (FBI) criminal history records is the level of access accorded for noncriminal justice purposes (e.g., equal to that of a private company doing an employment check on a new applicant, according to TSA) which limits TSA in accessing certain criminal history data related to charges and convictions. While TSA is seeking criminal justice type access to FBI systems, the FBI reports that it is legally unable to provide this access. The FBI and TSA are collaborating on options, but have not identified the extent to which a potential security risk may exist under the current process, and the costs and benefits of pursuing alternatives to provide additional access. Second, TSA officials reported the agency was not reviewing some state-provided criminal history for HME applicants because TSA did not have a mechanism to efficiently capture the data in its case system. Identifying a solution may help TSA better identify HME applicants posing security threats. Third, the TSA Adjudication Center relies on contractors for adjudicating applicant cases, and contractor turnover has affected the agency's ability to meet its growing workload. Developing a workforce staffing plan that considers the costs and benefits of using contractors will help ensure that TSA meets its growing credentialing workload.

---

# Contents

---

Letter		1
	Background	8
	Stakeholder Roles and Responsibilities Vary under TSA Credentialing Programs, and Nonfederal Entities Have Implemented Additional Requirements	13
	TSA Faces Data and Staffing Challenges in Ensuring Effectiveness of its Security Threat Assessments of Transportation Workers	28
	Conclusions	41
	Recommendations for Executive Action	42
	Agency Comments and Our Evaluation	42
Appendix I	Objectives, Scope, and Methodology	46
Appendix II	TSA Credentialing Programs	51
Appendix III	TSA TWIC, HME, and Aviation Workers Programs: Legislative Background and Purpose	53
Appendix IV	Criminal Offenses That May Disqualify Applicants from Acquiring a TWIC or HME	55
Appendix V	Criminal Offenses That Disqualify Applicants under the Aviation Workers Program from Acquiring an Airport-Issued Access Badge	58
Appendix VI	Comments from the Department of Homeland Security	61
Appendix VII	GAO Contact and Staff Acknowledgments	66

---

---

Tables

Table 1: Selected Characteristics of the 11 Selected Maritime Ports with State or Local Credentialing Programs	19
Table 2: Four Selected States Conducting Criminal History Record Checks on HME Applicants	26
Table 3: TSA Credentialing Programs	51
Table 4: Legislative Background and Purpose of TSA's TWIC, HME, and Aviation Workers Programs	53

---

Figures

Figure 1: Comparison of TSA and Nonfederal Governing Entity Roles with Respect to the TWIC, HME, and Aviation Workers Programs	15
Figure 2: Average Monthly Program Enrollment and TTAC Adjudication Center Caseload for Reviewing Applicants with Potentially Disqualifying Information for TWIC, HME, and Aviation Workers Programs—July 2010 through June 2011	39

---

---

### Abbreviations

ATSA	Aviation and Transportation Security Act
Compact Act	National Crime Prevention and Privacy Compact Act
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
HME	Hazardous Materials Endorsement
MTSA	Maritime Transportation Security Act
NCIC	National Crime Information Center
SIDA	Security Identification Display Area
TSA	Transportation Security Administration
TTAC	Transportation Threat Assessment and Credentialing
TWIC	Transportation Worker Identification Credential

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



G A O

Accountability \* Integrity \* Reliability

United States Government Accountability Office  
Washington, DC 20548

---

December 8, 2011

The Honorable John D. Rockefeller IV  
Chairman  
The Honorable Kay Bailey Hutchison  
Ranking Member  
Committee on Commerce, Science,  
and Transportation  
United States Senate

The Honorable Peter T. King  
Chairman  
The Honorable Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security  
House of Representatives

Securing transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and international commerce. Since 9/11, the Transportation Security Administration (TSA) within the Department of Homeland Security (DHS) has taken steps to ensure that transportation workers, particularly those that transport hazardous materials or have unescorted access to secure areas of federally regulated maritime or airport transportation facilities are properly screened to ensure they do not pose a security threat.<sup>1</sup> These efforts are intended to reduce the probability of a successful terrorist or other

---

<sup>1</sup>Under Coast Guard maritime security regulations, a secure area, in general, is an area over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard-approved security plan. For most maritime facilities, the secure area is generally any place inside the outer-most access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. Secured airport areas include those portions of an airport, specified in the airport security program, for which security measures are conducted and generally include three categories. In general (1) a Security Identification Display Area (SIDA) is an area in which appropriate identification must be worn, (2) a sterile area provides passengers access to boarding aircraft and is an area to which access is generally controlled by TSA or a private screening entity under TSA oversight, and (3) an Air Operations Area is an area providing access to aircraft movements and parking areas. See 49 C.F.R. § 1540.5.

---

criminal attack on the nation's transportation systems, which include approximately 360 ports and more than 450 commercial airports.

TSA reported administering 17 transportation security related credentialing programs covering a population of approximately 15 million transportation workers such as those accessing airports and maritime ports, as well as truckers seeking a hazardous materials endorsement to a commercial driver's license. These 17 TSA credentialing programs include conducting applicant background checks—known as Security Threat Assessments—which are TSA reviews of applicant information and searches of government databases to determine if the applicant has known ties to terrorism and meets specified requirements such as those relating immigration status and criminal history.<sup>2</sup> In addition, pursuant to federal law and corresponding regulations, TSA requires that airport and aircraft operators ensure that individuals undergo a fingerprint-based criminal history records check and terrorism and immigration checks, before receiving identification credentials that enable them unescorted access to SIDA or sterile areas of the airport.<sup>3</sup> Most TSA credentialing programs are administered internally with no equivalent nonfederal government entity (namely states or port authorities) responsibilities under federal regulations.<sup>4</sup> However, for 3 of 17 TSA programs, nonfederal government entities have certain responsibilities under federal statutes and corresponding regulations, such as for enrolling applicants or issuing credentials to workers. These 3 programs are as follows:

---

<sup>2</sup>A Security Threat Assessment includes conducting a background check to determine whether each applicant is a security risk to the United States. These checks, in general, can include checks for criminal history records, immigration status, terrorism databases and watchlists, and records indicating an adjudication of lack of mental capacity, among other things. TSA security threat assessment-related regulations define the term security threat to mean an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

<sup>3</sup>See 49 U.S.C. § 44936; 49 C.F.R. §§ 1542.209, 1544.229 and 1544.230.

<sup>4</sup>For example, in accordance with Coast Guard regulation, all mariners employed aboard U.S. merchant vessels greater than 100 Gross Register Tons (Domestic Tonnage), except operators of uninspected passenger vessels, are required to have a valid U.S. Merchant Mariners Credential. Under this program, TSA and Coast Guard conduct the background check, with Coast Guard responsible for issuing a credential. Once the credential is issued, the Coast Guard is responsible for verifying the validity of the credential. Nonfederal public entities—such as a state or port authority—do not have roles in this credentialing process. Port authorities may be state or local government entities, but may also be privately operated.

- 
- **TSA’s Transportation Worker Identification Credential (TWIC) Program:** A program requiring TSA to complete a Security Threat Assessment on individuals requiring unescorted access to secure or restricted areas of maritime facilities regulated under the Maritime Transportation Security Act (MTSA) of 2002<sup>5</sup> and to issue a TSA biometric credential to qualified individuals.<sup>6</sup>
  - **TSA’s Hazardous Materials Endorsement (HME) Threat Assessment Program:** A program requiring TSA to conduct a Security Threat Assessment on truckers who apply for a Hazardous Materials Endorsement to a state commercial driver’s license.
  - **TSA’s Aviation Workers Program:** A program requiring TSA to complete a Security Threat Assessment and airport operators to complete a criminal history record check on individuals who apply for or are issued a credential for unescorted access to secure areas in U.S. domestic airports, including airport facility workers, retail employees, and airline employees.

Federal statutes and corresponding regulations relating to the TWIC, HME, and Aviation Workers programs generally do not preempt nonfederal governing entities from implementing additional nonconflicting requirements. As a result, the number of credentialing programs in place by TSA, and the potential for their redundancy with nonfederal governing entity programs, has raised questions as to whether transportation workers may be subject to redundant background checks with different standards and additional costs.

Section 817 of the Coast Guard Authorization Act of 2010<sup>7</sup> mandated that we review background checks and forms of identification required under state and local transportation security programs and assess whether these programs duplicate or conflict with federal programs. The act also mandated that we make recommendations to the House Committee on Homeland Security and the Senate Committee on Commerce, Science,

---

<sup>5</sup>Pub. L. No. 107-295, 116 Stat. 2064, 2073-74 (2002).

<sup>6</sup>Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

<sup>7</sup>Pub. L. No. 111-281, 124 Stat. 2905, 2999 (2010).



---

and Transportation on steps that can be taken to reduce or eliminate the duplication with federal programs. To fulfill this requirement, we addressed the following questions:

- What are the roles and responsibilities of federal and nonfederal government entities related to certain TSA transportation worker credentialing-related programs and how do selected nonfederal governing entities' credentialing programs compare to TSA's programs?
- What challenges, if any, does TSA face in ensuring the effectiveness of its credentialing-related programs?

To identify which DHS credentialing programs for transportation workers have requirements for state and local governments, we analyzed relevant federal laws, including pertinent sections, as amended, of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001,<sup>8</sup> the Aviation and Transportation Security Act,<sup>9</sup> and MTSA, plus relevant DHS regulations that set out corresponding requirements for TSA and nonfederal governing entities with respect to conducting background checks and issuing identification to transportation workers. On the basis of this information, we focused our analysis on comparing nonfederal transportation worker credentialing programs with TSA's TWIC, HME, and Aviation Workers programs. Only the TWIC, HME, and Aviation Workers programs include nonfederal governing entity responsibilities with respect to TSA programs.

To identify the roles and responsibilities of federal and nonfederal government entities related to certain TSA transportation security credentialing-related programs and how selected nonfederal governing entities' credentialing programs compare to TSA's programs, we examined TSA documentation on the TWIC Program, HME Program, and Aviation Workers Program. We also interviewed officials at TSA, the DHS Screening Coordination Office<sup>10</sup>, the Coast Guard, the Federal Bureau of

---

<sup>8</sup>Pub. L. No.107-56, 115 Stat. 272, 396 (2001).

<sup>9</sup>Pub. L. No. 107-71, 115 Stat. 597, 639-40 (2001).

<sup>10</sup>The Screening Coordination Office was established by DHS to coordinate the numerous and disparate credentialing and screening initiatives within DHS.

---

Investigation (FBI), and the Department of Transportation (DOT) to discuss their role and nonfederal government entity roles in TSA transportation worker credentialing programs. We also interviewed officials from nine stakeholder organizations that represent the broad spectrum of nonfederal governing entity interests in TSA's programs, as well as officials from state and local governing agencies at selected maritime ports, airports, and state agencies to obtain their perspectives on TSA and nonfederal government roles and responsibilities.<sup>11</sup>

We collected information from maritime port authorities at 17 maritime port locations—including the top 10 ports by container volume in 2010—plus 7 additional ports we identified as having credentialing programs. We visited officials at five locations (Baltimore, Maryland; Norfolk, Virginia; Miami and Port Everglades, Florida; and New York, New York), based on whether a state or local port authority had in place a credentialing program outside of TSA's TWIC program. We also collected information from eight category X<sup>12</sup> airports—this included 4 of the top 6 airports by passenger boardings in 2009 plus four additional airports based on proximity to GAO offices.<sup>13</sup> We conducted site visits to three of these eight airports (Seattle-Tacoma International Airport, Washington Dulles International Airport, and Baltimore-Washington International Airport). Further, we collected information on state requirements for issuing hazardous material endorsements to commercial driver's licenses from licensing agencies in six states, including the top five states as ranked by commercial drivers license issuance based on DOT data as of December 2010, plus one additional state that we identified as having additional

---

<sup>11</sup>These organizations included the American Association of Port Authorities, Owner Operator Independent Drivers Association; American Trucking Associations; American Association of Motor Vehicle Administrators; American Association of Airport Executives; Institute of Makers of Explosives; National Petrochemical & Refiners Association; International Liquid Terminals Association; and the Agricultural Retailers Association.

<sup>12</sup>TSA classifies the nation's approximately 450 commercial airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings, and Category IV airports have the smallest.

<sup>13</sup>We obtained information from eight airports, including: Hartsfield-Jackson Atlanta International Airport, Los Angeles International Airport; Denver International Airport; John F. Kennedy International Airport; Seattle-Tacoma International Airport; Washington Dulles International Airport; Baltimore/Washington International Airport; and Portland International Airport.

---

state requirements.<sup>14</sup> To determine how nonfederal governing entities' credentialing programs compare to TSA's programs, we analyzed pertinent federal laws and regulation which authorize the TWIC, HME, and Aviation Workers programs, such as MTSA and the USA PATRIOT Act, as well as TSA policy documents for implementing the programs, such as operational guidance and policies. By reviewing these laws, regulations, and policies, we identified requirements of TSA and select state and local governing agencies, as well as applicant eligibility standards such as lists of disqualifying criminal offenses and duration of time that agencies were required to consider these disqualifying criminal offenses ("look back period"). We then compared these standards and practices with those implemented under nonfederal governing agency (state or local) programs we identified. While the information we obtained from selected nonfederal governing entities cannot be generalized across all states and localities, it provided us with a perspective on how state and local government transportation worker programs compare with federal programs and requirements.

To obtain information on challenges, if any, TSA faced in ensuring the effectiveness of its credentialing-related programs, we reviewed our reports, and analyzed pertinent laws and regulations related to TSA's use of criminal history record information, as well as TSA program documentation, including program training manuals, staffing information, and other documents detailing program processes and challenges TSA faced, for the TWIC, HME, and Aviation Workers credentialing programs. We also reviewed TSA data on the number of enrollments and adjudication caseload for TSA's TWIC, HME, and Aviation Workers programs—covering the period of July 2010 through June 2011. Through interviews with knowledgeable TSA officials we determined that these data were sufficiently reliable for our purposes. We interviewed headquarters officials from TSA's Transportation Threat Assessment and Credentialing (TTAC) program<sup>15</sup>, DHS' Screening Coordination Office,

---

<sup>14</sup>We obtained information from six states: California, Florida, Illinois, Maryland, New York, and Texas.

<sup>15</sup>On September 27, 2011, TSA announced a reorganization that would place TTAC into a newly established Office of Intelligence and Analysis. According to TSA, the agency is making several enhancements to better align headquarters functions to enable its continued evolution to a high performance counterterrorism organization. This includes merging various TTAC functions with the Office of Intelligence to ensure vetting and intelligence informs daily operations.

---

and the FBI's Criminal Justice Information Services Division, which maintains the FBI's national criminal history repository. Further, we reviewed cases from selected nonfederal governing entities of applicants whom entities had reported denying credentials, and the reasons they had done so. Additionally, we interviewed nonfederal agency stakeholders, including officials from two organizations representing state criminal justice repository agencies—the National Crime Prevention and Privacy Compact Council<sup>16</sup> (Compact Council) and SEARCH.<sup>17</sup> We then evaluated TSA credentialing program processes against TSA's credentialing program mission needs and *Standards for Internal Control in the Federal Government*<sup>18</sup> The information we obtained through our interviews with nonfederal government entities and stakeholder organizations are not generalizable, but provided valuable perspectives related to TSA's TWIC, HME, and Aviation Workers programs. Appendix I contains a more detailed discussion of our objectives, scope and methodology.

We conducted this performance audit from February through November 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

<sup>16</sup>The Compact Council's mission statement provides that the Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and security of society while recognizing the importance of individual privacy rights.

<sup>17</sup>SEARCH is a nonprofit organization created by and for states which serves as the national consortium for justice information and statistics. It is governed by a Membership Group comprised of one gubernatorial appointee from each of the 50 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands, as well as eight at-large appointees selected by SEARCH's Chair. Members are primarily state-level justice officials responsible for operational decisions and policymaking concerning the management of criminal justice information, particularly criminal history information.

<sup>18</sup>GAO, *Standards for Internal Control in the Federal Government*, GAO.AIMD-00-21.3.1 (Washington, D.C.: November 1999).

---

## Background

---

### TSA Transportation Worker Credentialing Programs

TSA's credentialing programs are focused on identifying security threats posed by those individuals seeking to obtain an endorsement, credential, access and/or privilege (hereafter called a credential) for unescorted access to secure or restricted areas of transportation facilities at maritime ports and airports, or for transporting hazardous materials. TSA's 17 transportation security credentialing programs cover a population of approximately 15 million transportation workers in the maritime, surface, and aviation transportation modes. See appendix II for a table summarizing TSA credentialing programs.

Most of the TSA credentialing programs are administered internally to TSA agencies with no equivalent nonfederal government entity responsibilities under federal regulations. In this way, there would not be potential for redundancy or duplication between DHS and nonfederal governing entity functions. Only the TWIC, HME, and Aviation Workers programs include nonfederal governing entity responsibilities with respect to TSA programs. Appendix III summarizes the legislative background and purpose of these three programs.

As of June 2011, TSA reports that, collectively, the TWIC, HME, and Aviation Workers programs accounted for a population of approximately 4.4 million workers—about 30 percent of the population TSA has vetted through its 17 credentialing-related programs. The criteria TSA uses in its Security Threat Assessments for TWIC and HME applicants vary from that of the Aviation Workers Program. For example, Security Threat Assessment criteria are aligned under both the HME and TWIC programs. These criteria include 24 disqualifying criminal offenses categorized into 10 “permanent disqualifying criminal offenses” and 14 “interim disqualifying criminal offenses.”<sup>19</sup> Four of the permanent disqualifying criminal offenses, such as an act of terrorism and

---

<sup>19</sup>In addition, the TWIC and HME disqualifying criminal offenses include related conspiracy and attempt offenses for each of the 24 specified offenses.

---

espionage, are not eligible for waiver.<sup>20</sup> The other 20 disqualifying criminal offenses (6 permanent and 14 interim) are eligible for waiver. Interim disqualifying criminal offenses are those specified offenses for which an individual has either been convicted, or found not guilty by reason of insanity during a 7-year period prior to the application, or for which an individual was released from incarceration during a 5-year period prior to the application. In contrast, under the Aviation Workers Program, there are 28 disqualifying criminal offenses, but no permanent disqualifiers.<sup>21</sup> More specifically, disqualifying criminal offenses under the Aviation Workers Program are those for which an individual has been convicted, or found not guilty by reason of insanity during the 10 years prior to an application for airport identification. See appendix IV for a description of these disqualifying criminal offenses for the HME and TWIC programs and appendix V for these disqualifying criminal offenses for the Aviation Workers Program.

---

## TSA Credentialing-Related Processes

TSA's TTAC is responsible for administering Security Threat Assessments for transportation workers seeking to obtain a credential.<sup>22</sup> This includes ensuring only eligible individuals are granted TSA-related credentials, such as a TWIC, or a TSA Security Threat Assessment approval for a nonfederal governing entity to issue an identification badge or endorsement, such as an HME on a Commercial Driver's License. While TSA's transportation worker credentialing-related programs include varying purposes, standards, or agency responsibilities, they generally include some or all of following process components:

---

<sup>20</sup>Applicants with certain permanent disqualifying criminal offenses and any interim disqualifying criminal offenses may request a waiver of their disqualification. In general, TSA may issue such a waiver if TSA determines that an applicant does not pose a security threat based upon the security threat assessment. There is also an appeals process by which any applicant may appeal a TSA finding that the applicant poses a security threat.

<sup>21</sup>Similar to the TWIC and HME disqualifying criminal offenses, the aviation disqualifying criminal offenses also include additional related conspiracy and attempt offenses for each of the disqualifying offenses.

<sup>22</sup>The mission of TTAC is to reduce the probability of a successful terrorist or other criminal attack on the transportation system through the application of threat assessment methodologies that are intended to identify known or suspected terrorist threats working or seeking to access the United States' transportation system.

- 
- **Enrollment**—Applicants pay an enrollment fee and submit biographic (name, address, etc.) and biometric information (photo and fingerprints) to TSA or nonfederal governing entity.
  - **Background checking**—Security Threat Assessment processes include reviewing information to determine if applicants are disqualified to possess a credential based on criminal offenses, immigration eligibility issues, links to terrorism, or mental capacity, all varying by program. Criminal history record checks, which are fingerprint-based, require an adjudicator to review the applicant’s criminal history (referred to as a rap sheet) that occurred within a designated time frame (or look-back period) and compare this information against a set of disqualifying criminal offenses identified in statute and corresponding regulations in order to make a determination of eligibility. There are two levels of the Security Threat Assessment:
    - **Initial automated vetting.** The initial automated vetting process is conducted to determine whether any derogatory information is associated with the name and fingerprints submitted by an applicant during the enrollment process. This check is to be conducted against the FBI’s criminal history records. These records contain information from federal, state and local sources in the FBI’s National Crime Information Center (NCIC) database and the FBI’s Integrated Automated Fingerprint Identification System/Interstate Identification Index, which maintain criminal records and related fingerprint submissions.<sup>23</sup> The FBI’s criminal history records check is a negative identification check, whereby

---

<sup>23</sup>The FBI maintains the Integrated Automated Fingerprint Identification System, which is a national fingerprint and criminal history system that responds to requests from local, state, and federal agencies. The system provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. A segment of this system is the FBI-maintained criminal history record repository, known as the Interstate Identification Index (III or “Triple I”) system that contains records from all states and territories, as well as from federal and international criminal justice agencies. The state records in the III are submitted to the FBI by central criminal record repositories that aggregate criminal records submitted by most or all of the local criminal justice agencies in their jurisdictions. The records in the system are all based on 10 rolled fingerprints, which provide a positive, biometric match between the individual and his or her record. The NCIC is a name and biographic descriptor-based computerized system containing criminal justice information (i.e. wanted person information; sex offender information; missing person information; unidentified person information; and stolen property information).

---

the fingerprints are used to confirm that the associated individual is not identified as having a criminal record in the database. If an individual has a criminal record in the database, the FBI provides a criminal history rap sheet to TSA for adjudication. A check is also conducted against federal terrorist identity information from the Terrorist Screening Database, including the Selectee and No-Fly lists.<sup>24</sup> To determine an applicant's immigration/citizenship status and eligibility, TSA also checks applicant information against the Systematic Alien Verification for Entitlements system.<sup>25</sup> If the applicant is a U.S.-born citizen with no related derogatory information, the system can approve the individual's application for a credential with no further review of the applicant or human intervention.

- **TSA's TTAC Adjudication Center Review.** A second-level review is conducted as part of an individual's background check if (1) the applicant has self-identified themselves to be a non-U.S. citizen or non-U.S. born citizen or national, or (2) the first-level review uncovers any derogatory information, such as a criminal offense. As such, not all applicants will be subjected to a second-level review. The second-level review consists of staff at TSA's Adjudication Center in Herndon, Virginia reviewing the applicant's enrollment file to determine if derogatory information may be potentially disqualifying.

---

<sup>24</sup>Pursuant to Homeland Security Presidential Directive 6, dated September 16, 2003, the Terrorist Screening Center—under the administration of the FBI—was established to develop and maintain the U.S. government's consolidated database of terrorist screening information, called the Terrorist Screening Database. Terrorist identity information in the Terrorist Screening Database is used for security-related screening processes. The Selectee List, a subset of the Terrorist Screening Database, contains information on individuals who must undergo additional security screening before being permitted to board an aircraft. The No Fly List, another subset of the Terrorist Screening Database, contains information on individuals who are prohibited from boarding an aircraft. The No Fly and Selectee lists contain applicable identity information from the Terrorist Screening Center's consolidated database of known or suspected terrorists.

<sup>25</sup>Run by U.S. Citizenship and Immigration Services, the Systematic Alien Verification for Entitlements information system is an intergovernmental initiative designed to aid benefit-granting agencies in determining an applicant's immigration status, thereby ensuring that only entitled applicants receive federal, state, or local public benefits and licenses. The program is an information service for benefit-granting agencies, institutions, licensing bureaus, and other governmental agencies.



- 
- **Credential Issuance**—involves the issuance of a physical card or endorsement.
  - **Verification**—refers to the responsibilities of the credential holder as well as the responsibilities of those entities which have regulatory responsibility for ensuring that only credentialed workers can perform certain functions or access secure or restricted areas of transportation facilities. This includes making a determination that the credential presented is authentic (not fraudulently developed); that the individual is the one to whom the document was issued (not an impostor), and remains valid (not revoked or expired).
  - **Renewal**—requires applicants to re-enroll, undergo a new Security Threat Assessment, and obtain a new credential.
  - **Revocation**—refers to the ability of the issuing entity to physically and/or electronically revoke a credential. Authority for revocation (such as TSA or a state or local government entity) varies pursuant to federal regulations for each credential program.

---

## Regulations Concerning Federal Preemption of State and Local Credentialing Requirements

In general, TSA credentialing regulations related to programs with state and local government involvement do not preempt state and local governments from implementing their own background checking or badging system requirements. For example, the TWIC final rule noted that TSA has asserted preemption in some areas “where federal regulations have historically dominated the field, such as merchant mariner regulations” but not with respect to state “background checks or badging systems in addition to the TWIC.” According to the rule, states may be the proprietor of ports or port facilities, and as the proprietors they are free to set standards determining who may enter their facilities, as does any other proprietor. The TWIC rule further provided that (1) states may have set standards for reasons other than guarding against the threat of terrorism, such as to combat drug smuggling or organized crime, and (2) as such, they are not regulating in the same areas that DHS is regulating. In addition, TSA’s 2004 Interim Final Rule for the HME program recognized that the state is the licensing body for drivers who are state residents, and that the state has a clear mandate and interest in protecting the residents and drivers within its borders from dangerous drivers. As a result, TSA asserted that it did not wish to preclude additional state measures applied to drivers by the state as long as such measures are not inconsistent with the TSA rule. In this way, a state may conduct background checks using information from the state’s criminal

---

history repository and/or add additional disqualifying offenses.<sup>26</sup> However, according to the TSA Interim Rule, a state would be preempted from applying a standard in which the federal interim disqualifying offenses are no longer treated as disqualifying. Similarly, airports have generally not been preempted from instituting additional background checks beyond those required by federal regulation and TSA's Aviation Workers Program, as part of their security plan and credentialing program.

---

## Stakeholder Roles and Responsibilities Vary under TSA Credentialing Programs, and Nonfederal Entities Have Implemented Additional Requirements

---

### Stakeholders Have Varying Roles and Responsibilities in Credentialing

TSA conducts a Security Threat Assessment for those enrolled in its TWIC, HME, and Aviation Workers programs, but state and local governing entities' roles and responsibilities in these programs vary by program. For example, TSA is responsible for implementing the entire TWIC credentialing process including enrollment, background checks and credential issuance, with no role for maritime port facility operators—be they public port authority or privately operated facilities—outside of verifying credentials that have been issued. In contrast, under the Aviation Workers Program, TSA and airports and aircraft operators each have certain responsibilities for several elements of the credentialing process, including the criminal history record check. For example, airports and aircraft operators are responsible for ensuring the collection of application information, enrolling applicants and transmitting the results to

---

<sup>26</sup>Each state maintains a central criminal repository, or database, of criminal arrests and convictions of individuals in that state.

---

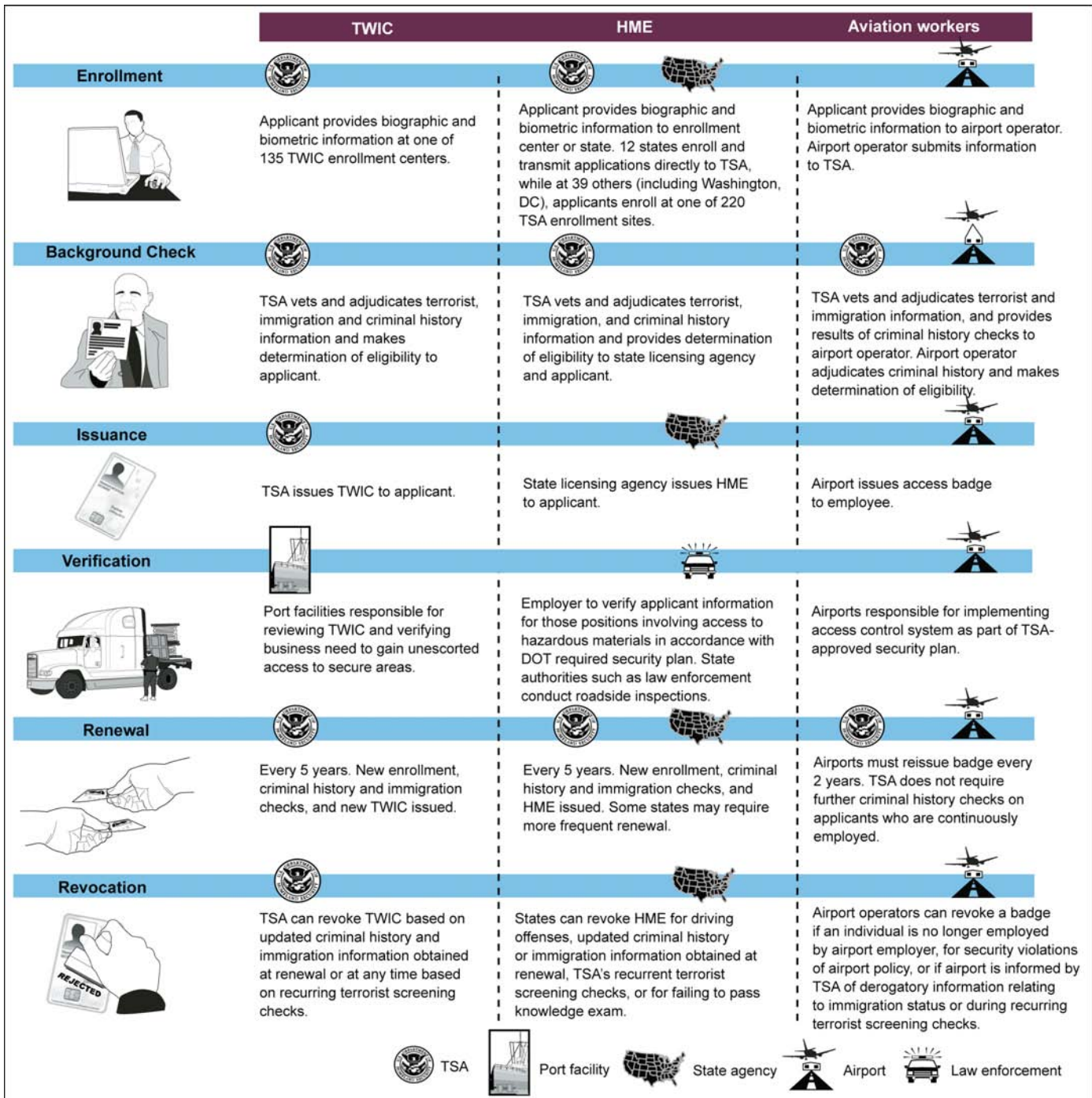
TSA for the Security Threat Assessment. TSA's roles include TSA adjudicating the immigration and terrorism checks, running automated FBI criminal history records, and transmitting the results of the criminal history record checks to the airports and aircraft operators, which have a responsibility under TSA regulations for adjudicating the criminal history to identify potentially disqualifying criminal offenses specified under TSA regulations, and making a final determination of eligibility.<sup>27</sup> Moreover, airport and aircraft operators issue their own local identification badges.

Figure 1 summarizes the credentialing processes for the TWIC, HME, and Aviation Workers programs and the respective responsibilities of TSA, nonfederal governing entities, and private entities under these TSA programs.

---

<sup>27</sup>Individuals with unescorted access to an airports Sterile Area and SIDA are required to undergo immigration and terrorist vetting as well as a criminal history record check. Those requiring Air Operations Area access undergo a terrorist and immigration check, but not a criminal history record check.

**Figure 1: Comparison of TSA and Nonfederal Governing Entity Roles with Respect to the TWIC, HME, and Aviation Workers Programs**



Source: GAO analysis of DHS, DOT, and state information. Art Explosion (clipart).

---

## Nonfederal Governing Entities Have Additional Credentialing Requirements Compared to TWIC and HME

### Maritime Port Programs

Port authorities or state agencies at 11 of the 17 maritime ports we contacted—including 4 of the top 10 largest maritime ports—had implemented additional credentialing requirements to those of the TWIC program.<sup>28</sup> Of these 11 maritime ports, 10 required employer sponsorship in addition to a valid TWIC, 3 required applicants to undergo additional criminal history record checks, and 10 issued a local port identification credential in addition to the TWIC which was necessary for gaining unescorted access to secure areas of MTSA regulated port facilities. The following highlights key elements of these programs.

- **Enrollment.** In addition to collecting biometric and/or biographic information from applicants, ports with additional programs required applicants to have a valid TWIC and generally required employer sponsorship as prerequisites for obtaining a local port credential. In general, sponsorship included requirements for applicants to provide documentation of port employment, such as a letter with an authorized employer signature, which the governing entity verifies. For example, at the port of Norfolk, the Virginia Port Authority requires all facility operators to register with local law enforcement, and once registered, these facilities are authorized to submit applications on behalf of employees who require access. In general, the programs had aligned their renewal requirements with those of the applicant's TWIC. For example, if an applicant has 3 of the 5 years of eligibility remaining on their TWIC, then the local credential would need to be renewed after 3 years.
- **Background Checks.** At 3 of 11 ports that had additional requirements, governing entities were conducting additional criminal history record checks, while two others—the Port of Miami and Port Everglades—had discontinued conducting additional criminal history record checks in May 2011 in addition to the federal-level checks TSA

---

<sup>28</sup>Based on information we obtained between April and November 2011.

---

used as part of its Security Threat Assessment for TWIC.<sup>29</sup> First, whereas TSA's criminal history record check is conducted based on searches of the FBI's national databases, the governing entities for these three ports conduct both state and FBI criminal history record checks.<sup>30</sup> State repositories are considered more comprehensive sources of state criminal history than that maintained by FBI databases. Second, one port governing agency considered additional disqualifying criminal offenses beyond those stipulated in TSA regulations that may disqualify applicants from acquiring the local port identification. For example, the Waterfront Commission of New York Harbor was screening applicants against additional disqualifying offenses, including theft and burglary, as did the two Florida ports prior to the repeal of Florida's state criminal history record check requirement for seaport employees.

- **Issuance.** We found the types of credential issued under local programs had similar characteristics, with some ports reporting plans to change or eliminate their physical credentials as part of a future TWIC reader system deployment. For example, 10 of 11 ports with additional credentialing programs had requirements in place for an individual to obtain and present a second, locally issued port identification for unescorted access to port facilities—in addition to a TWIC. Of these, 9 ports reported using machine-readable credentials as part of their access control systems.<sup>31</sup> For example, at the Port of

---

<sup>29</sup>In May 2011, the State of Florida amended Florida State Law 311.12 repealing provisions requiring workers accessing the state's 12 active deepwater public ports to undergo a state criminal history records check. The repealed provisions contained disqualifying offenses, such as theft and burglary, not specifically identified as a disqualifying offense under the TWIC program. The repealed provisions also required that individuals who had obtained their TWIC through the federal TWIC-waiver process, whereby individuals with disqualifying offenses could be granted a TWIC, had to additionally seek a Florida waiver. While Florida has repealed its background check requirements, various Florida ports still require that individuals attempting to gain access to a port or facility provide a local port-specific identification card in addition to the TWIC.

<sup>30</sup>Each state maintains a repository, which is a central database that maintains criminal history records on all state offenders. Records include fingerprint files and files containing identification segments and notations of arrests and dispositions. The central repository is generally responsible for state-level identification of arrestees, and commonly serves as the central control terminal for contact with FBI record systems.

<sup>31</sup>A machine readable identification card can be read with or without direct contact (proximity) of the card with an electronic reader. Techniques for storing and reading the cards include smart chips which are integrated circuits imbedded in the card which allow data to be stored on the card, bar codes, and magnetic strips.

---

Wilmington, North Carolina, the North Carolina State Port Authority issues a local identification access card which is a machine-readable card with a smart chip that contains some personal information, such as a name and picture. In addition to verifying that a cardholder's identification is valid for access to secure or restricted areas of the port facility, some entities had designed their systems to provide access control capabilities within the port facility so that only those populations of workers authorized to enter certain facilities within the port were able to do so. Unlike TWICs that cannot be customized by port facilities, some port-specific cards were color coded to signify areas which cardholders were authorized to access.

Six of 11 port authorities reported plans to revise or do away with their credentialing programs once the Coast Guard issues its final reader rule for the TWIC program and the ports deploy readers for electronically verifying TWICs.<sup>32</sup> For example, in 2011, the South Carolina Port Authority reported it was planning to eliminate its physical identification card for the Port of Charleston and adopt a program whereby the port's central database ties worker enrollment information with individuals' TWIC information. Under this system, the port authority will upload permission to different access points which will be read by card readers and will verify whether a TWIC is active.<sup>33</sup>

Table 1 summarizes the key aspects of the 11 ports with additional credentialing requirements.

---

<sup>32</sup>To date, Coast Guard has not issued its final TWIC card reader rule. The Coast Guard is responsible for developing TWIC-related security regulations and ensuring that MTSA-regulated maritime facilities and vessels are in compliance with these regulations. In August 2006, DHS officials decided, based on industry comment, to implement TWIC through two separate regulations, or rules. The first rule, issued in January 2007, directs the use of the TWIC as an identification credential or flashpass. The second rule, the card reader rule, is currently under development and is expected to address how the access control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC. On March 27, 2009, the Coast Guard issued an Advance Notice of Proposed Rule Making for the card reader rule.

<sup>33</sup>TSA maintains a database identifying whether a TWIC is valid or has been cancelled. TSA provides MTSA regulated port facility operators with periodic updates of this information.

**Table 1: Selected Characteristics of the 11 Selected Maritime Ports with State or Local Credentialing Programs**

Port with state or local government program <sup>a,b</sup>	State criminal history record check	Applicant fee	Local port credential issued
Alabama State Port Authority (Mobile)	yes	\$25	yes
Port Everglades <sup>c</sup>	none (authorizing law repealed May 2011)	none <sup>d</sup>	yes
Georgia State Port Authority (Port of Savannah)	none	none	yes
Maryland Port Administration (Port of Baltimore)	none	none	yes
Massachusetts Port Authority (Port of Boston)	none	none	yes
Port of Miami <sup>c</sup>	none (authorizing law repealed May 2011)	none	yes
Port of New York/New Jersey <sup>e</sup>	yes	\$25 for truck driver credential, \$66.30 to \$94.20 for longshoreman background check <sup>f</sup>	yes
North Carolina State Ports Authority (Port of Wilmington, Morehead City)	yes	\$20	yes
Port of Portland (Oregon)	none	none	yes
South Carolina State Ports Authority (Charleston) <sup>g</sup>	none	none	no
Virginia Port Authority (Norfolk, Newport News, Portsmouth)	none	none	yes

Source: GAO analysis of selected maritime port credentialing program information.

<sup>a</sup>As reported between April and November 2011.

<sup>b</sup>Covered populations include longshoremen, truck drivers, and other workers including contractors, vendors, shipping personnel, and any persons regularly accessing restricted areas of the marine terminals.

<sup>c</sup>On May 24, 2011, Florida repealed, among other things, the portions of state law 311.12, which had required the state to conduct FBI and state criminal history record checks of all individuals seeking unescorted access to restricted and secure areas within the state's 12 active deepwater ports. These provisions of the Florida state law had been in place since 2000. According to a Port Everglades official, under this state program applicants were required to pay fees of \$50 that included the criminal history record check and an administrative fee.

<sup>d</sup>Port Everglades does not charge a fee for TWIC holders to obtain a port credential. Port Everglades also issues credentials (with a fee of \$25) to those individuals who work only in a supportive or administrative position within port offices and do not access secure or restricted areas of the port.

<sup>e</sup>Two separate governing agencies implement the background check and identification programs for workers seeking access to facilities at the Port of New York/New Jersey. The Waterfront Commission of New Harbor, a bi-state government agency, conducts criminal history record checks and issues an identification card to longshoremen seeking access to work at port facilities in New York and New Jersey. The Port Authority of New York/New Jersey does not conduct criminal history record checks on workers seeking access. However, the port authority requires truckers seeking access to register in its truck driver identification system, known as Sealink, and to obtain machine-readable identification cards.



---

<sup>f</sup>The Waterfront Commission of New York Harbor conducts state and FBI criminal history record checks on all longshoremen seeking a Waterfront Commission License, which is required to access Port of New York and New Jersey facilities. The Waterfront Commission charges varying fees to applicants depending upon whether they are New Jersey or New York residents. This includes \$44.30 in New Jersey and \$72.20 in New York to cover the costs of the respective state. An additional \$22 is charged to cover the cost of an FBI national criminal history check.

<sup>g</sup>Previously, at the Port of Charleston, the South Carolina Port Authority charged an applicant a fee of \$20 for enrollment and identification costs. However, a port official reported that the port had transitioned away from a physical card. Instead, the port had installed TWIC readers and was tying the applicant enrollment information to the TWIC card.

**Benefits of Maritime Programs.** Officials at ports with credentialing programs reported their programs were providing additional security benefits to those of the TWIC program. In particular, ports most commonly cited the following security benefits of their local credentialing programs:

- **Mechanism for Establishing Business Need:** Governing officials from 10 of 11 ports with additional programs reported that their local enrollment and identification served as a mechanism for establishing a valid business reason for an individual to access the secure or restricted areas of the port facility, in accordance with TSA and Coast Guard requirements. As discussed, under Coast Guard regulations, the possession of a TWIC itself is not sufficient to gain unescorted access to a secure area of a MTSA-regulated port facility—a facility operator must also ensure the applicant is authorized to be in the area.<sup>34</sup> Because 10 of the 11 ports were requiring employer sponsorship, ports were using their enrollment and identification cards as a method for determining this business need. In this way, these local credentials are serving a purpose not included under TSA’s TWIC enrollment process because—as we reported in May 2011—TSA’s TWIC enrollment process does not require employer sponsorship.<sup>35</sup> Instead, applicants attest to their need for a TWIC via their signature on the application.

---

<sup>34</sup>The method by which facility operators may meet this requirement is left to the operator themselves, such as by questioning TWIC holders to determine whether they have a bonafide business need.

<sup>35</sup>GAO, *Transportation Worker Identification Credential, Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*. [GAO-11-657](#) (Washington, D.C.: May 10, 2011).

- 
- **Denying Credentials to Criminals:** Governing officials from the five ports with active or prior background check requirements cited benefits their local programs provide over TWIC to control and monitor access to individuals with criminal history. For example, maritime port authorities seek to limit crime in their ports and thus officials from two ports reported that they required additional scrutiny of all TWIC holders who reported receiving their TWIC through the TWIC waiver process. The TWIC waivers enabled applicants with certain interim disqualifying criminal offenses, such as murder or unlawful weapons possession, to obtain a TWIC.<sup>36</sup> For example, the Port of Miami, Port Everglades, and the Alabama State Port Authority provided us with a sample of individuals who had either been denied local credentials or had local credentials revoked.<sup>37</sup> We provided TSA 30 of these names to confirm that they had valid TWICs. In 11 of the 30 cases, TSA adjudicators identified disqualifying criminal offenses but the applicants were ultimately approved for a TWIC through the redress process (waiver or appeals). Among those offenses committed by these 11 individuals were murder, attempted murder, carjacking and armed robbery, and unlawful possession of a firearm.

In addition, officials from three ports reported criminal history record checks enabled them to target local risks facing their ports which are not addressed under TSA regulations for the TWIC program. For example, officials from the Port of Miami and the Waterfront Commission of New York Harbor told us that, while they recognized the threats posed by terrorism, crime was a major concern for their ports, particularly narcotics

---

<sup>36</sup>Under TSA's Security Threat Assessment process, applicants who are determined to have disqualifying criminal offenses may request a waiver for certain disqualifying offenses, including murder and robbery. Appendix IV lists these offenses. MTSA required the establishment of a waiver process, and under TSA implementing regulations, TSA may issue a waiver if TSA determines that an applicant does not pose a security threat after considering, as applicable, the circumstances of the disqualifying act or offense, restitution made by the applicant, and federal or state mitigation remedies, court records, or official medical release documents indicating that the applicant no longer lacks mental capacity, or other factors that indicate the applicant does not pose a security threat warranting denial.

<sup>37</sup>TSA reported all were valid TWIC holders as of July 1, 2011.

---

trafficking and cargo theft.<sup>38</sup> Officials reported that by screening applicant criminal history records against certain additional disqualifying offenses to those of TWIC, such as theft, they were able to deny access to a population of felons they perceived as longstanding criminal risks facing the port who might be granted a TWIC. These governing entities reported denying credentials to applicants who had been granted TWICs. For example, between January 2009 and May 2011, the Port of Miami reported it had denied credentials to 101 applicants, including 52 valid TWIC holders.<sup>39</sup> Port Everglades also reported it had denied credentials to applicants, including those with valid TWICs. Among those denied, was an individual convicted for conspiracy to possess with intent to distribute cocaine in 2007, yet issued a TWIC in 2010. According to these Port Everglades documents, this individual was arrested several times for other offenses, such as unlawful possession of a firearm, including a short-barrel shotgun and machine gun, and other narcotics offenses.

Further, the three ports reported that they had mechanisms in place for conducting recurring criminal history checks on an ongoing basis through an automated “rap back” program.<sup>40</sup> Specifically, the Waterfront Commission of New York Harbor, which conducts background checks for longshoremen at the Port of New York/New Jersey, has a mechanism in place that allows it to receive automated notifications on arrests and warrants. According to officials at the Waterfront Commission of New York Harbor, these notifications have led to the suspension and revocation of numerous longshoremen credentials. Examples from local credentialing programs of those who had TWICs but were denied by selected governing port authorities after local disqualifying criminal offenses were committed include the following:

---

<sup>38</sup>Concern over the impact of illicit drugs and drug trafficking came to the forefront in Florida during the mid to late 1990s. According to a 1998 Florida State Senate report, Florida ports had extensive criminal networks conducting narcotics and cargo theft. According to this report, in 1997 there were more cocaine-related deaths in Florida than murders. Additionally, the FBI estimates that in the United States, cargo theft amounts to \$12 billion annually and finds that most cargo theft occurs in or near seaports.

<sup>39</sup>According to Port of Miami officials, many of the 52 TWIC holders were denied because they had disqualifying criminal offenses based on the former state port security law, including for multiple theft violations.

<sup>40</sup>A rap back refers to an automated system identifying arrests, wants, or warrant information of an individual after compiled criminal history information has been released to a requesting agency.

- 
- An individual issued a TWIC in 2008, who was subsequently convicted of robbery and grand theft in 2010. The individual's local credential was revoked in December 2010. TSA identified this individual as having a valid TWIC as of July 2011.
  - **Greater Access Control Than TWIC:** At 9 of the 11 ports with additional programs, officials reported that having a local credential that could be verified by an existing access control system provided them the capability to better verify the card presented, while more quickly and effectively canceling access control to workers who violate security procedures. For example, a Florida port reported it revoked the local identification card of an individual because it had been notified by state law enforcement of the arrest of the cardholder for possession with intent to distribute cocaine. Officials noted that their programs were particularly important in verifying TWIC cardholders because the Coast Guard had yet to issue a final rule laying out requirements for electronic verification of TWICs.

**Costs of Maritime Programs.** Some of the 11 ports with separate credentialing programs imposed additional costs. The costs were largely associated with administering the credentialing program. For the ports that charged a fee, the applicants were required to pay these fees in addition to their credentialing costs already incurred in obtaining their TWIC.<sup>41</sup> We found that the nonfederal governing entities were charging applicant fees at 3 of 11 ports, ranging from \$20 to \$94.20. For these ports, applicant fees were generally covering costs for administering state and national FBI criminal history record checks. We found the fees among these ports differed based on the varying costs charged by governing entities for conducting the criminal history checks and whether an FBI criminal history record check was also required. For example, the Alabama State Port Authority conducts state criminal history record checks, and charges applicants a fee of \$25 to cover the administrative costs for these checks and its port identification credential. According to the Alabama State Port Authority, applicant fees covered 70 percent of the costs of its program, with the remainder funded by operating

---

<sup>41</sup>TSA requires TWIC applicants pay a fee of \$132.50 pursuant to 6 U.S.C. § 469, which requires TSA to charge reasonable fees for credentialing and background investigations in the field of transportation.

---

revenues.<sup>42</sup> Another agency, the Waterfront Commission—which requires applicants to successfully undergo a criminal history record check to obtain a license and credential authorizing their access to Port of New York and New Jersey facilities—charges applicants fees of up to \$94.20 to cover the costs of both the FBI criminal history record check and either a New York or New Jersey criminal history records checks depending upon the applicant being a resident of New York or New Jersey.

Labor and industry organizations have for several years raised concerns over the costs imposed by federal, state and local port requirements. For example, the International Longshoreman's Association has expressed concerns that allowing states to impose different requirements requiring multiple identification cards forces workers to go through additional review processes, and paperwork, and costs place an unfair burden on port workers, who would face redundant clearance processes. Other organizations, including the American Trucking Associations and the Owner-Operator Independent Drivers Association, have also raised cost concerns, particularly in that workers may be required to pay applicant fees to obtain multiple federal credentials. For example, with respect to federal requirements alone, generally a truck driver hauling hazardous materials is required to obtain a HME (\$89.25 for TSA-managed states and more depending on state), and may also be required to obtain a TWIC (\$105.25, if an applicant already has a HME) if he or she sought access to a MTSA-regulated port facility. Depending on the port, a local credentialing requirement may add an additional cost to the worker. TSA is reportedly developing new regulations in addition to a technical solution to help reduce redundancies in TSA's Security Threat Assessment processes under its Transportation Infrastructure Modernization program.<sup>43</sup>

---

<sup>42</sup>The Alabama State Port Authority reported costs including an NCIC subscription for conducting name based criminal history checks and classroom supplies for required security awareness training required for applicants.

<sup>43</sup>TSA established the Infrastructure Modernization program to standardize and consolidate the agency's Security Threat Assessment systems. We are currently conducting a separate review of this program and anticipate reporting by the end of calendar year 2011.

---

## HME and Aviation Workers Credentialing Programs

**HME Issuance by State Licensing Agencies.** Under federal law and corresponding TSA regulations, states are prohibited from issuing a commercial drivers license with a hazardous materials endorsement to an individual unless TSA first conducts a Security Threat Assessment and determines that the individual does not pose a security risk. We found that four of the six states we contacted conducted additional state criminal history record checks on HME applicants, in addition to the national FBI criminal history record checks TSA conducted.<sup>44</sup> Of these four states, three—Florida, Texas, and Maryland—were submitting the results to TSA for further review and action. These three states were not adjudicating the results of these criminal history checks, but sending the information to TSA as part of its HME Security Threat Assessment.<sup>45</sup> The other state, New York, was the only selected state which conducted a separate vetting program for HME applicants.<sup>46</sup> For example, in accordance with New York state law, New York state is required to conduct both a state criminal history check and an FBI criminal history check on all HME applicants. In addition, New York State’s program includes additional disqualifying criteria beyond the HME related disqualifying criminal offenses considered under the TSA Security Threat Assessment. For example, New York’s consideration of additional disqualifying criminal offenses not covered by TSA regulations includes larceny and burglary. The four states conducting criminal history record checks charged applicants additional fees as part of enrollment to cover the cost of required state criminal history record checks—ranging from \$15 to \$75. Table 2 summarizes the four selected states with additional background checking activities and requirements.

---

<sup>44</sup>Of the six states that we contacted, the four that conducted state criminal history record checks were Florida, Maryland, New York, and Texas. Two others contacted—California and Illinois—reported not implementing additional activities.

<sup>45</sup>Two of these four states—New York and Maryland—are required by state statute to conduct state criminal history checks on applicants before issuing a HME. The two others—Texas and Florida—both reported they were doing so on a voluntary basis.

<sup>46</sup>According to responsible officials with New York state’s program, New York state’s lawmakers established their program to address the unique security threats facing New York.

**Table 2: Four Selected States Conducting Criminal History Record Checks on HME Applicants**

Selected state <sup>a</sup>	Additional disqualifying offenses to TSA	Different look-back period than TSA	Additional applicant cost for state criminal check
Florida	none	no	\$36
Maryland	none	no	\$42
New York	yes	10 years	\$75
Texas	none	no	\$15

Source: GAO analysis of state information.

<sup>a</sup>As reported between March and September 2011.

**Airports.** The eight airports we contacted reported they did not conduct additional background checks beyond those required by TSA—which includes adjudicating the results of FBI criminal history record checks TSA provided. Unlike with the TWIC and HME programs, local authorities (airport operators and aircraft operators) are responsible for adjudicating the results of TSA-provided criminal history identified through automated FBI criminal history checks rap sheet, to determine whether applicants had potentially disqualifying offenses. In doing so, the airports may follow up with an applicant if the FBI rap sheet TSA provided lacks a disposition of a criminal offense—which is necessary for the airports to determine if the applicant has potentially disqualifying criminal offenses. Although not required by TSA all of these airports required employer sponsorship to verify the employment of applicants and their need to access certain areas of the airport. In addition, unlike the TWIC program where only TSA can revoke a TWIC, under the Aviation Workers program airport authorities are the entities that revoke an airport issued credential—not TSA.<sup>47</sup> For example, airports are to revoke a worker’s identification badge if TSA determines a badgeholder poses a threat and may also do so if a worker violates airport security policy.

<sup>47</sup>If TSA determines that an individual poses a threat based on checks of information in the Terrorist Screening Database or immigration checks, TSA will notify the airport to revoke the credential.

---

Unlike the TWIC and HME programs which require new fingerprint-based criminal checks as part of the renewal process<sup>48</sup>, TSA regulations for airport operators do not require additional criminal history checks of workers with authorized access authority as long as workers maintain continuous employment with the same issuing authority. However, although not required by TSA regulation, some airports we contacted reported conducting fingerprint-based criminal history record checks on a random basis to identify potentially disqualifying criminal offenses that the identification holder may have committed since the initial Security Threat Assessment was conducted.

In general, TSA credentialing-related regulations do not preempt state and local background checks or credentialing programs. Both maritime port authorities and state licensing agencies have implemented credentialing programs with requirements beyond those of TSA's TWIC and HME programs. While these programs have included additional costs to applicants, they have also provided nonfederal governing entities with additional tools for identifying potential threats and restricting access not offered under TSA's credentialing programs. Thus, these credentialing programs complement, rather than duplicate, the TSA programs we reviewed.

---

<sup>48</sup>TWICs, in general, are to expire 5 years after the date of issuance at the end of the calendar day. With respect to HMEs, each state must require that hazardous material endorsements be renewed every 5 years or less so that individuals are subject to a TSA security screening requirement at least every 5 years.



---

## TSA Faces Data and Staffing Challenges in Ensuring Effectiveness of its Security Threat Assessments of Transportation Workers

---

### Additional Criminal History Record Information Could Strengthen TSA's Security Threat Assessments

Criminal history record checks are a key element of the Security Threat Assessment process for TSA's credentialing programs, helping to ensure that the agency detects those applicants with potentially disqualifying criminal offenses. As discussed earlier, TSA's criminal history record check compares an applicant's name and fingerprints against criminal history record information provided by the FBI, including from the FBI's National Crime Information Center and Interstate Identification Index.<sup>49</sup> However, according to TSA, the access the agency currently has to criminal history information for making its eligibility determinations for its credentialing programs—including TWIC, HME, and Aviation Workers—has limitations.

TSA reports that it has been difficult to effectively and efficiently conduct Security Threat Assessment adjudication of criminal history records due to the limited access it has as a noncriminal justice purposes requestor of

---

<sup>49</sup>The Interstate Identification Index system uses an index-pointer approach to tie together the criminal history record databases of state central repositories and the FBI. Under this system, the FBI makes available an index listing the names of individuals on whom it maintains criminal history record information. An agency seeking criminal history record information on a specific individual will submit that individual's name and fingerprints to the FBI. The Bureau will match the name and fingerprints against the index and then "point" the information request to the database (either State or Federal) where the requested information is maintained. The index contains information on persons arrested for fingerprintable felonies and misdemeanors under state or federal law. It includes identification information (for example, name, birth date, race and gender), and FBI and state identification numbers from each state that has information about an individual. FBI reports the Integrated Automated Fingerprint Identification System, which includes the Interstate Identification Index, held the criminal histories of more than 70 million subjects.

---

criminal history records—and that this limitation had increased the risk that the agency was not detecting potentially disqualifying criminal offenses. Specifically, the level of access through which TSA receives criminal history record information through the FBI’s Interstate Identification Index is the level of access accorded for noncriminal justice purposes. According to TSA, this level of access only allows a limited view of criminal history record information as opposed to a more expanded level of access accorded criminal justice agencies. The terms “noncriminal justice purposes” and “criminal justice” in this context, stem from the National Crime Prevention and Privacy Compact Act of 1998 (Compact Act).<sup>50</sup> The Compact Act, enacted in 1998, in general, organizes an electronic information-sharing system among the federal government and the states to exchange criminal history records for noncriminal justice purposes authorized by federal or state law. The Compact Act also established a Compact Council with the authority to promulgate rules and procedures governing the use of the Interstate Identification Index system for noncriminal justice purposes, not to conflict with FBI administration of the Interstate Identification Index for criminal justice purposes.<sup>51</sup> The Compact Act contains, among others, the following definitions:

- Noncriminal justice purposes: The term noncriminal justice purposes means “uses of criminal history records for purposes authorized by Federal or state law other than purposes relating to criminal justice activities, including employment suitability,

---

<sup>50</sup>Pub. L. No. 105-251, 112 Stat. 1870, 1874 (1998). According to Compact Council documents, the Compact became effective April 28, 1999, after Montana and Georgia became the first two states to ratify it, respectively. To date, 29 states have ratified the Compact.

<sup>51</sup>The National Crime Prevention and Privacy Compact provides for the creation of a Compact Council to oversee noncriminal justice use of the Interstate Identification Index. The Compact Council’s mission statement provides that the Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and security of society while recognizing the importance of individual privacy rights. Under the Compact Act, the 15 members of the Compact Council appointed by the Attorney General are to be comprised of nine State Compact Officers, two at-large members nominated by the FBI Director, two at-large members nominated by the Chairman of the Compact Council, one FBI Advisory Policy Board representative, and one FBI representative.

---

licensing determinations, immigration and naturalization matters, and national security clearances.”

- Criminal justice: The term criminal justice “includes activities relating to the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history records.”<sup>52</sup>

As an agency categorized with a “noncriminal justice purposes” level of access to criminal history records information, TSA reports receiving limited access to certain types of criminal history data. For instance, when TSA sends the FBI its fingerprint submissions for credentialing program applicants, the FBI responds to TSA with criminal history record information including federal-level criminal history information, as well as state-level criminal history records obtained from any of the 15 states that participate in the FBI’s National Fingerprint File Program.<sup>53</sup> As a noncriminal justice agency, TSA reports that its access to state criminal history information from other states is more limited than the level of access available to criminal justice agencies which provides access to criminal history record information from all 50 states plus the District of Columbia. Thus, TSA reports that its visibility to applicant criminal history records is often incomplete because the provided information excludes details regarding dispositions, sentencing, release dates, and probation or

---

<sup>52</sup>In addition, the Compact Act defines the term “criminal justice agency” to mean, (1) courts, and (2) a governmental agency or subunit thereof that (i) performs the administration of criminal justice pursuant to a statute or executive order, and (ii) allocates a substantial part of its annual budget to the administration of criminal justice. The term criminal justice agency also includes federal and state inspectors general offices.

<sup>53</sup>All 50 states and the District of Columbia participate in the Interstate Identification Index. Fifteen states also participate in the National Fingerprint File. National Fingerprint File states assume responsibility for providing Interstate Identification Index-indexed records for criminal and noncriminal requests—a responsibility traditionally maintained by the FBI. Since states traditionally report to have more complete information than what has been submitted to the FBI’s systems, the National Fingerprint File allows participating states to provide their state rap sheets directly when the FBI processes fingerprint-based criminal history record checks. The FBI reports that, as of October 9, 2011, the 15 National Fingerprint File states were Colorado, Florida, Georgia, Hawaii, Idaho, Kansas, Maryland, Minnesota, Montana, North Carolina, New Jersey, Oklahoma, Oregon, Tennessee, and Wyoming.

---

parole violations, among others. TSA reported that this lack of visibility to additional criminal history record information via the FBI's Interstate Identification Index system hinders its ability to fulfill its homeland security mission and conduct Security Threat Assessments with more detailed and complete information for its credentialing programs.<sup>54</sup>

According to a 2006 Department of Justice report<sup>55</sup> while the FBI's Interstate Identification Index is comprehensive in its coverage of nationwide arrest records for serious offenses, it is still missing final disposition information for approximately 50 percent of its records.<sup>56</sup> For example, the FBI reported that information states submitted into its systems was not always complete or current and that state repositories often reported having more complete or current information than what was forwarded to and maintained in FBI systems.<sup>57</sup> As a result, state criminal history repositories contain records, such as arrests and convictions, not included—or indexed—as part of the FBI's databases. For this reason, according to the 2006 Department of Justice report, checks of state databases, in addition to an FBI check, are considered necessary to get more comprehensive data.

---

<sup>54</sup>According to TSA, the agency has conducted over 3 million Security Threat Assessments requiring a criminal history record check, and over 40 percent of the cases have included associated criminal records identified during automated FBI database checks, thus requiring an initial manual review by adjudicators at the TTAC Adjudication Center.

<sup>55</sup>U.S. Department of Justice, Office of the Attorney General, *The Attorney General's Report on Criminal History Background Checks* (June 2006).

<sup>56</sup>According to a TSA estimate from November 2010, of the 3 million Security Threat Assessments requiring a criminal history record check, over 40 percent of the cases had associated criminal records that TSA manually adjudicated for possible disqualifying offenses. Of these, TSA's TTAC issued 62,000 initial threat determinations for applicants identified with potentially disqualifying offenses. Of these, roughly 23,560 (38 percent) had open dispositions and TSA reported that many of these may have been resolved through expanded criminal justice information access to FBI's Interstate Identification Index.

<sup>57</sup>The FBI reported that, to address the issue, the Bureau had historically taken a proactive approach to encourage and assist agencies to submit complete and accurate information in a timely manner. Among these efforts have included providing operational and policy guidance to agencies requesting assistance with submitting criminal history record information, hosting annual national criminal history improvement conferences, technical support to agencies transitioning from manual processing to automated electronic submissions.

---

According to TSA, being provided “noncriminal justice purposes” level of access also affects its ability to run the FBI database checks using the fingerprints collected at enrollment on a recurring basis to identify potentially disqualifying criminal history of an active credential holder. Under the Compact Act, subject fingerprints or other approved forms of positive identification must be submitted with all requests for criminal history record checks for “noncriminal justice purposes.”<sup>58</sup> Thus, to conduct fingerprint-based check on an ongoing basis for previously approved individuals, TSA would have to submit prints and pay a fee to the FBI (funded by an applicant fee) each time it wanted to have a criminal history record check run.<sup>59</sup> According to DHS Screening Coordination Office officials, all of the agency’s credentialing programs which include a criminal history record check have weaknesses similar to what we reported in our May 2011 report on the TWIC program. In that report, we stated that TSA’s controls for TWIC were not designed to determine whether TWIC holders have committed disqualifying crimes at the federal or state level after being granted a TWIC.<sup>60</sup> In particular, we noted that TSA conducts criminal history record checks only during enrollment or a name-based check of TWIC holders against federal wants and warrants on an ongoing basis, but it did not run the broader FBI fingerprint based check using fingerprints collected at enrollment on an ongoing basis.<sup>61</sup>

TSA has noted that it does not fit neatly into a criminal justice or noncriminal justice definition and asserts that its Security Threat Assessments require both criminal justice and noncriminal justice

---

<sup>58</sup>Compact Act implementing regulations provide that for purposes approved by the Compact Council, a delayed submission of fingerprints may be permissible under exigent circumstances.

<sup>59</sup>The Departments of Commerce, Justice, and State, and Related Agencies Appropriations Act, 1991, in general, authorizes FBI to establish and collect fees to process fingerprint identification records and name checks for non-criminal justice purposes, and the current FBI fee is \$17.25 per check (Pub. L. No. 101-515, 104 Stat. 2101, 2112 (1990)(codified at 28 U.S.C. §534 note)).

<sup>60</sup>[GAO-11-657](#).

<sup>61</sup>TSA reported that it conducts a name-based check of enrollees against federal wants and warrants on an ongoing basis for TSA credentialing programs which require a criminal history record check. However, these checks are against federal wants and warrants lists, not state-level information. Federal wants generally consist of information on wanted persons, or individuals, for whom federal warrants are outstanding.

---

functions.<sup>62</sup> Within this context, TSA is seeking an expanded level of access to FBI's Interstate Identification Index system data, beyond a "noncriminal justice purposes" level of access, to a level of access similar to that accorded criminal justice agencies. TSA's position, in general, is that the Compact Act definitions of "criminal justice" and "noncriminal justice purposes" do not mandate that TSA Security Threat Assessment functions only be accorded a noncriminal justice purposes level of access. With respect to the term "noncriminal justice purposes," it is TSA's position that its statutorily mandated Security Threat Assessments are not the same as employment or licensing background suitability checks listed in the "noncriminal justice purposes" definition. TSA's position is that its obligation to detect individuals with specific convictions to minimize the threat to transportation systems require greater access to the FBI's data.

The FBI's position, in general, is that TSA is not a criminal justice agency, that the functions it performs are "noncriminal justice" in nature, and that, as such, based upon a plain reading of federal law, the FBI cannot legally provide TSA with criminal justice access to criminal history records information. The FBI notes that the Compact Act specifically defined "noncriminal justice purposes" as "uses of criminal history records for purposes authorized by Federal or State law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances." It is the FBI's position that TSA's requests for criminal history record information fall within this "noncriminal justice purposes" definition and, as such, the FBI is not authorized to provide TSA with criminal justice access to criminal history record information. FBI additionally notes that a broad interpretation of the Compact Act outside of its plain meaning would violate the Compact Act related laws of the 29 states that have signed the Compact as well as the contractual agreement that the United States Government entered into with these states.

---

<sup>62</sup>According to TSA, it is not by definition a criminal justice agency, but is uniquely different in scope and nature of mission. Security Threat Assessments, according to TSA, are not uniquely noncriminal justice in nature, as they are not employment specific, but the goal of conducting them is to prevent, deter, and protect critical infrastructure and transportation networks against terrorist attacks.

---

TSA is collaborating with the FBI and the Compact Council to identify possible options for obtaining greater access to criminal history record information for its Security Threat Assessments. Since 2010, TSA has made several presentations to members of the Compact Council seeking a criminal justice-like access to FBI databases. While the FBI and Compact Council have not agreed with TSA's position seeking a level of access similar to that accorded criminal justice agencies, the FBI has taken steps to provide TSA access to criminal history related information. In particular, FBI reported pursuing technical solutions that would expand the extent of state level criminal history available to TSA—as well as to other federal agencies classified as noncriminal justice agencies that may seek criminal history access through FBI's systems. For example, as a longer-term technical solution scheduled to be operational in 2014, FBI is planning to enhance its Integrated Automated Fingerprint Identification System to allow for automated noncriminal justice access to obtain additional information from 36 states, including the 15 National Finger Print File states and an additional 21 states.

The FBI, as an interim technical solution, reported plans to provide federal agencies improved functionality similar to its longer-term plan. The FBI reports that a pilot for this program was to begin in October 2011 with TSA serving as the first participating federal agency.<sup>63</sup> According to an FBI study, these technical solutions may provide TSA with additional criminal history information for roughly 15 percent of its credentialing program applicant population. However, TSA reported that while such an enhancement would be an improvement from current processes, a substantial amount of state's records will remain inaccessible.

According to *Standards for Internal Control in the Federal Government*, effective internal controls provide for an assessment of the risks the agency faces from both internal and external sources. Management must decide upon internal control activities required to mitigate those risks and achieve the objectives of efficient and effective operations. As part of this, management should design and implement internal controls that are informed by the identified risks the program faces, the possible effect of those risks, control activities required to mitigate those risks, and the

---

<sup>63</sup>The FBI reports that this solution would provide TSA with additional information to support TSA adjudication determinations, including information on the offense level type and the specific state statute of the offense.

---

costs and benefits of mitigating those risks.<sup>64</sup> TSA and the FBI have shared goals in detecting potential terrorist and criminal threats posed to the nation's transportation facilities. The agencies have continued a dialogue on options, and the FBI is implementing technical solutions which may improve the criminal history information available to TSA. However, the two agencies have not jointly determined the extent to which a potential security risk may exist with respect to the level of access to criminal history records information that TSA currently receives to complete Security Threat Assessments. Conducting such an assessment which leverages ongoing coordination with the Compact Council, would help address potential security risks that may exist with respect to the level of access to criminal history record information currently received by TSA for conducting Security Threat Assessments, and could be used to help inform discussions about possible alternatives to address any risks, and the costs and benefits of pursuing each alternative.

---

### TSA Could Better Leverage Available State Criminal History Data

TSA could further strengthen its Security Threat Assessment process by leveraging certain existing flows of state criminal history information already provided by some nonfederal governing entities for its HME program. As discussed earlier, four of the states we contacted reported conducting their own state criminal history record checks for applicants seeking an HME. Three of these four states reported sending the results of their state criminal history checks directly to TSA for consideration as part of its Security Threat Assessments—Florida, Texas, and Maryland. However, TSA HME program officials reported that the agency had generally not reviewed and considered the state-provided criminal history information from all of these states.

TTAC officials acknowledged that the additional information they were receiving from some states may help the agency identify potentially disqualifying offenses among HME applicants. However, TSA reported that it has not established a mechanism to efficiently capture the information from all of the states that were directly providing the information. For example, the TTAC Adjudication Center uses a web-enabled system—known as its Screening Gateway—as its primary tool

---

<sup>64</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).



---

for gathering, viewing, and synthesizing applicant case information for each Security Threat Assessment. In this way, all vetting information is compiled into a single case record for adjudicator review. For example, TSA has in place a mechanism for Florida to transmit applicant state criminal history results electronically to TSA for adjudication, but it does not have such a mechanism to electronically capture the information from other states providing the information.<sup>65</sup> TSA officials reported that reviewing the information outside of its web-based case system would be time consuming and result in delays in processing the Security Threat Assessment adjudication caseload—which TSA officials noted was over 12,000 cases per month for the HME program alone.

According to TSA records, the agency has met with officials from states that directly provided criminal history records information to discuss the technical steps that would be necessary for them to send TSA criminal history information in a manner that TSA may effectively use. According to TSA documentation, as of March 2010 TSA reported that more research was necessary to identify technical steps necessary to achieve a solution that would allow TSA to leverage the directly-provided criminal history information.

TSA reported it has sought possible solutions to receive data directly from other states in an automated solution. However, the agency has faced obstacles because states have varying data systems and legal and practical constraints requiring TSA to develop unique solutions for obtaining data from a state. As a result, TSA reported it was pursuing a common technical solution for obtaining state criminal information through the agency's TTAC Infrastructure Modernization Program. Nonetheless, TSA's schedule for the modernization program indicates that it will not be completed until late 2015 and TSA has yet to determine how the program would integrate existing streams of criminal history provided by states. Moreover, TSA reported that future efforts to obtain additional state criminal information may require TSA to pay additional fees to states and the cost of these fees may need to be funded by increasing applicant fees for TSA credentialing programs. However, not all states are currently charging TSA additional fees for the criminal history information they already provide. A senior official with the one state which provided TSA

---

<sup>65</sup>Officials with the Florida Department of Law Enforcement reported using a 2005 DHS grant to fund a technical solution for transmitting its information to TSA. Officials reported doing so to improve the information available for TSA's Security Threat Assessment.

---

criminal history record information reported that his agency continued to do so because of concerns that TSA was adjudicating HME applications without the benefit of criminal history information, and had offered to make its records available to TSA in a number of electronic formats.

*Standards for Internal Control in the Federal Government* highlights the need for capturing information needed to meet program objectives and assessing the risks agencies face. TSA has reported that it needs access to all credible, reliable, and current information possible to meet its mission requirements for its credentialing programs and has been impeded in doing so because it lacks access to state criminal history information. Reviewing these state-provided criminal history records may help TSA address this challenge. TSA reported that more research was required to determine a format for integrating the information, and implementing a solution would carry costs for the agency. Conducting and documenting an assessment of the risks associated with not using the information—which considers existing and potential technical and staffing requirements, as well as analyzing the costs and benefits of establishing a format to integrate the information—may help TSA mitigate its reported access limitations and better meet its mission needs.

---

## TTAC Adjudication Center Workforce Challenges

The TTAC Adjudication Center has been challenged to meet its workload requirements since it began conducting operations in 2005. According to the TTAC Adjudication Center's current staffing plan, last released in February 2011, insufficient federal staff has hampered the Adjudication Center's ability to meet its workload requirements and ensure necessary oversight of the credential decision-making process. Among other things, the plan states that staffing limitations had left the center unable to perform quality assurance and oversight responsibilities, conduct necessary redress activities, and issue "Initial Determinations of Threat Assessments" in a timely manner.<sup>66</sup> According to a senior TTAC Adjudication Center official, the Adjudication Center has faced recurring challenges in meeting its workload since it began operations—largely related to TSA's reliance on contractor staff as its primary adjudicator workforce. As of July 2011, 72 percent (38 of 53) of Adjudication Center

---

<sup>66</sup>If TSA determines an applicant has one or more disqualifying criteria, the agency issues an Initial Determination of Threat Assessment letter to the applicant. Redress is adjudication of cases for those applicants seeking a waiver or appeal to the Initial Determination of Threat Assessment.

---

staff were contractors.<sup>67</sup> The challenge is that TSA has used three different contractors since establishing the adjudication center in 2005, and on each occasion the turnovers have led to backlogs as the TTAC adjudication center hired and trained new staff.<sup>68</sup> According to the official, federal staff must train each new set of contractors, and it has taken about 8 to 10 months for new contractors to become proficient so they may assume their full responsibilities. Because the Adjudication Center relies on contract staff to adjudicate the majority of its caseload, the contractor turnover has required the federal staff to take on additional work during these periods. According to the Adjudication Center official, federal staff have needed to regularly work overtime over the past five years to meet workload requirements. The official also noted that, whereas there has been considerable turnover with respect to contractors, the Adjudication Center has seen little turnover among its federal staff, with only two federal adjudicators leaving the center since operations began.

According to TSA data for the period of July 2010 through June 2011, the TTAC Adjudication Center adjudicated an average of approximately 36,000 cases a month involving TWIC, HME, and Aviation Workers Program applicants, including initial cases where automated background check results included potentially derogatory information and redress cases, such as applicant requests for a waiver or appeal to a prior determination.<sup>69</sup> Figure 2 shows the average monthly enrollment and TTAC Adjudication Center caseload for the TWIC, HME, and Aviation Workers programs—July 2010 through June 2011.

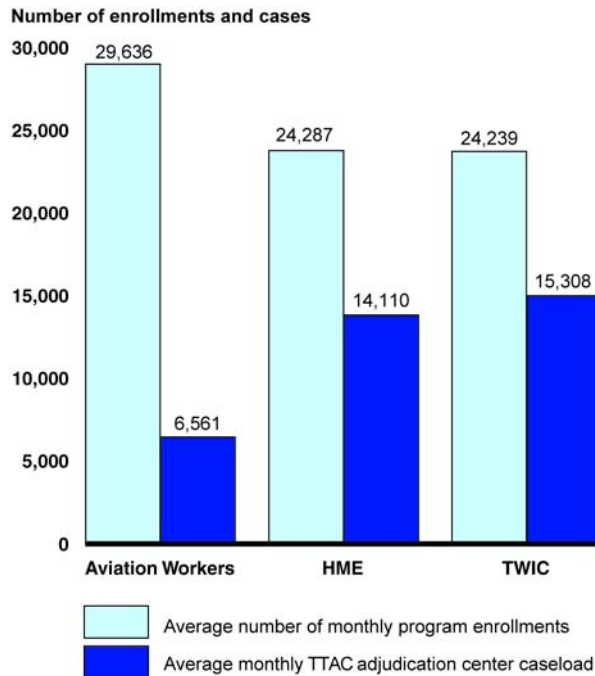
---

<sup>67</sup>The Adjudication Center caseload is completed using contractor staff to perform initial adjudication with federal staff reviewing all potentially disqualifying cases, issuing Initial Determination of Threat Assessments, and conducting redress actions supported by more senior contractor staff.

<sup>68</sup>TSA reported that upon the completion of each existing contract period of performance, the government was required to resolicit for a new contractor.

<sup>69</sup>According to TSA data, a total of 937,933 applicants enrolled in TSA's HME, TWIC, and Aviation Workers programs from July 2010 through June 2011. During automated vetting, 396,514 applicants were identified as having some derogatory information requiring adjudication center review during this period.

**Figure 2: Average Monthly Program Enrollment and TTAC Adjudication Center Caseload for Reviewing Applicants with Potentially Disqualifying Information for TWIC, HME, and Aviation Workers Programs—July 2010 through June 2011**



Source: GAO analysis of TSA data.

TSA reported that it chose to use contract adjudicators when the Adjudication Center was created because it considered them to be the most readily available workforce and the most effective way to augment federal staff with skilled resources. We have previously reported that to mitigate risks associated with using contractors, agencies have to understand when, where, and how contractors should be used given the risk of diminished institutional capacity, potentially greater costs, and mission risks.<sup>70</sup> Further, in July 2009, through its Balanced Workforce Strategy, DHS instructed

<sup>70</sup>GAO, *A model of Strategic Human Capital Management*, [GAO-02-373SP](#) (Washington, D.C.: Mar. 15, 2002).

---

components to review current contracts to determine if inherently governmental work was included in the work requirements.<sup>71</sup>

TSA awarded a new adjudication center contract in February 2010 that runs through January 2015. This contract includes a 1-year base period with four, 1-year options. Under this contract, based on the performance of the contractor, TSA may select another contractor within the next 5 years which could result in a change in its adjudicator workforce—and pose risks to the Adjudication Center’s sustainability and performance in meeting mission requirements.<sup>72</sup> Furthermore, TSA anticipates expanding the Adjudication Center caseload considerably for additional credentialing programs, which may further exacerbate these challenges.<sup>73</sup> Strategic workforce planning includes aligning an organization’s human capital program with its current and emerging mission and developing long-term strategies for acquiring, developing, and retaining staff to achieve these goals.<sup>74</sup> TSA reported that it initiated an assessment in March 2011 to determine if adjudication functions are appropriate to be performed by a contractor workforce, or if the work is inherently governmental and if there would be a cost savings resulting from conversion of the contract positions to government personnel. However, in September 2011, TSA reported that it did not have a date for when the study would be complete. Completing this assessment could help TSA address the risk that the agency may be using nonfederal employees to perform inherently governmental functions in its Adjudication Center. Moreover, the Adjudication Center’s most recent workforce staffing plan does not address issues related to its growing workload or the impact of the use of contractors for potentially inherently governmental functions. Updating its staffing plan to clarify how the Adjudication Center will effectively and efficiently meet its current and emerging workload requirements, based in part on the results of

---

<sup>71</sup>Inherently governmental functions are generally defined as those functions that are so intimately related to the public interest as to require performance by federal government employees.

<sup>72</sup>According to the contract, for the first year, contractor fees are \$5,954,821—of which \$4,463,918 is for labor.

<sup>73</sup>According to TSA’s contract for the Adjudication Center, taking on new programs may increase the caseload of the adjudication center—including doubling or tripling the caseload for some durations.

<sup>74</sup>GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning* [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003).

---

TSA's study, and developing timelines for doing so will help ensure that TTAC can effectively meet its growing workload.

---

## Conclusions

The state and local credentialing programs we reviewed complement, rather than duplicate, TSA's credentialing programs. In addition to working with state and local entities, TSA also works with the FBI to protect the nation's transportation systems from terrorist and criminal threats. Both agencies rely on timely, relevant criminal history data to do so. While TSA, the FBI, and Compact Council have collaborated on the issue, TSA and the FBI have not completed a joint analysis identifying whether a potential security risk may exist with TSA's present level of access to FBI criminal records as a "noncriminal justice purposes" requesting agency. Conducting an assessment which identifies the pros and cons of potential solutions to mitigate any potential risks could increase the rigor of the Security Threat Assessment, benefit federal and state decision-makers and better inform Congress about the potential weaknesses and their implications. Although TSA has reported seeking additional access to state-level criminal history, the agency has not leveraged some existing information it already receives directly from states. Conducting an assessment of the risks associated with not using the information, as well as the costs and benefits, such as technical barriers, to integrating the information into the current adjudication process, may help TSA strengthen its process and better meet its mission needs.

Since 2005, TSA's Adjudication Center has been responsible for ensuring that the millions of TSA credentialing program applicants do not pose a security risk to the United States, and these responsibilities are expected to grow considerably as TSA assumes additional responsibility for adjudicating Security Threat Assessments for additional credentialing programs which may double or triple its current workload. Thus, it is incumbent on TSA to complete its reported study to determine whether the use of contractors for its Adjudication Center is an inherently governmental function and if there would be a cost savings resulting from conversion of the contract positions to government personnel. Completing this assessment could help TSA address the risk that the agency may be using nonfederal employees to perform inherently governmental functions in its Adjudication Center. Moreover, updating its workforce staffing plan to define how the Adjudication Center will effectively and efficiently meet its current and emerging workload requirements, based in part on the results of TSA's study, and developing timelines for doing so, will help ensure that TTAC can effectively meet its current and growing workload.

---

## Recommendations for Executive Action

We recommend that the Secretary of Homeland Security direct the TSA Administrator, and the Attorney General of the United States direct the Director of the FBI, to jointly assess the extent to which a security risk may exist with respect to the level of access to criminal history records information currently received by TSA to complete Security Threat Assessments, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative.

We also recommend that the Secretary of Homeland Secretary direct the TSA Administrator to take the following two actions:

- Conduct an assessment of the risks associated with not utilizing some state-provided criminal history information, as well as an analysis of the costs and benefits of integrating the information into the current adjudication process.
- Develop a workforce staffing plan with timelines articulating how the TTAC Adjudication Center will effectively and efficiently meet its current and emerging workload requirements, and incorporate the results of TSA's study examining the appropriateness and costs and benefits of using contractors.

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS and DOJ for their review and comment. DHS, in written comments received November 30, 2011, concurred with all three of the recommendations in the report directed to DHS, and identified actions taken, planned, or under way to implement the recommendations. In an email received November 29, 2011, the DOJ audit liaison stated that DOJ concurred with the one recommendation we directed to DOJ in the report. Written comments are summarized below and official DHS comments are reproduced in appendix VI. In addition, both DHS and DOJ provided written technical comments, which we incorporated into the report, as appropriate.

In commenting on the draft report, DHS and DOJ described efforts the departments have underway or planned to address our recommendations. However, as discussed below, additional actions are needed to ensure that our recommendations are fully implemented. Both DHS and DOJ concurred with our first recommendation that the FBI and TSA jointly assess the extent to which a security risk may exist with respect to the level of access to criminal history records information currently received by TSA to complete Security Threat Assessments, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative.

---

DOJ stated that the FBI remains concerned that readers must understand that the level of access afforded to TSA to FBI criminal history records information for Transportation Worker Security Threat Assessments is one prescribed by law and not merely an opinion of the FBI's. DHS stated that it recognizes that there are criminal records at the state level which TSA does not receive, and noted that its level of criminal history information access is equal to that of a private company doing an employment check on a new applicant. DHS stated that it has been working with DOJ, the FBI and the states for several years to obtain more comprehensive access to criminal history record information, and cited plans for pilot programs with the FBI for accessing additional state criminal history records information—including a pilot to obtain information from over 20 additional states that respond to noncriminal justice requests through the FBI's Interstate Identification Index. DHS stated that as the pilots progress, TSA will work with the FBI to identify the differences between the standard FBI criminal history record information noncriminal justice results and the additional state data. DHS noted that TSA will work with the FBI to include these results in the overall assessment of risks regarding TSA's current level of criminal history record information access.

DHS also concurred with our second recommendation for TSA to conduct an assessment of the risks associated with not utilizing some state-provided criminal history information. DHS stated that while TSA concurred with the intent of the recommendation, it was no longer necessary to conduct a risk or cost and benefit analysis because it has identified a solution to incorporate state-provided criminal history records information into its adjudication process. Since DHS reported identifying this solution after we provided our draft report to the agencies for comment, we will continue to work with TSA to monitor progress on the proposed solution as it proceeds.

DHS concurred with our third recommendation that TSA develop a workforce staffing plan with timelines articulating how the TTAC Adjudication Center will effectively and efficiently meet its current and emerging workload requirements, and incorporate the results of TSA's study examining the appropriateness and costs and benefits of using contractors. DHS stated that it is currently meeting its Adjudication Center workload requirements and provided us with a copy of the workforce staffing plan. TSA stated that it recognizes the importance of appropriately balancing its federal and contractor workforce and in 2010 began a review to ensure that the right workforce balance is achieved. DHS stated that TSA is analyzing the results of this review to achieve the best balance of federal and contractor resources as part of the Department-wide Balanced Workforce Strategy, and that the results would be available once finalized.



---

Lastly, DHS noted that TSA would continue to assess the staffing needs of the Adjudication Center to implement emerging requirements based on the results of the Balanced Workforce Strategy. However, these actions do not fully address the intent of our recommendation. As we have noted, the staffing plan TSA provided cited challenges the Adjudication Center faced in meeting workload requirements—such as staffing limitations leaving the center unable to perform quality assurance and oversight responsibilities, conduct necessary redress activities, and issue “Initial Determinations of Threat Assessments” in a timely manner. Given the significant challenges cited, it is unclear whether TSA is fully meeting current Adjudication Center workload requirements. Since TSA reports it no longer faces challenges in meeting its workload, it will be important for TSA to update the February 2011 staffing plan TSA provided. Lastly, TSA reported that it began a review to determine that the right workforce balance is achieved. As discussed earlier, TSA reported this review is to determine if adjudication functions are appropriate to be performed by a contractor workforce, or if the work is inherently governmental and if there would be a cost savings resulting from conversion of the contract positions to government personnel. However, TSA has yet to complete this assessment nor provide timelines for doing so. Completing this study and incorporating the results of this assessment into an updated staffing plan remains important for TSA to help ensure it appropriately and effectively meets its Adjudication Center workload.

---

We are sending copies of this report to the Secretary of Homeland Security, the Assistant Secretary for the Transportation Security Administration, the Commandant of the United States Coast Guard, the Attorney General of the United States, the Director of the Federal Bureau of Investigation, and appropriate congressional committees. In addition, this report is available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions, please contact me at (202) 512-4379 or [lords@gao.gov](mailto:lords@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VII.

A handwritten signature in black ink that reads "Stephen Lord". The signature is written in a cursive, flowing style.

Stephen M. Lord  
Director  
Homeland Security and Justice Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

To identify the roles and responsibilities of federal and nonfederal government entities related to the Transportation Security Administration's (TSA) transportation security credentialing-related programs, we first identified those programs which place certain responsibilities on state and local governments. To do this, we analyzed relevant statutes, including pertinent provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001,<sup>1</sup> the Aviation and Transportation Security Act,<sup>2</sup> and the Maritime Transportation Security Act (MTSA)<sup>3</sup> of 2002, plus relevant Department of Homeland Security (DHS) regulations that set out corresponding requirements for TSA and nonfederal governing entities with respect to conducting background checks and issuing identification to transportation workers.

We also reviewed documentation provided by TSA, such as program summaries, which outlined the respective roles and responsibilities of federal and nonfederal governing entities under 17 different credentialing programs. On the basis of this information, we focused our analysis on comparing nonfederal transportation worker credentialing programs with three TSA credentialing programs—the Transportation Worker Identification Credential Program, Hazardous Materials Endorsement Program, and Aviation Workers Program—because they placed certain regulatory responsibilities on nonfederal governing entities. Of the 17 TSA credentialing programs, only the Transportation Worker Identification Credential (TWIC), Hazardous Materials Endorsement (HME) Threat Assessment, and Aviation Workers programs include nonfederal governing entity responsibilities.

We further examined TSA documentation describing, among other things, the roles and responsibilities of various entities for enrolling applicants, conducting background checks, and issuing credentials. We also interviewed headquarters and field officials at relevant agencies, including DHS (TSA, Screening Coordination Office, Coast Guard); Department of Justice Federal Bureau of Investigation (FBI) and Department of Transportation (DOT). In addition, we interviewed officials from nine

---

<sup>1</sup>Pub.L. No.107-56, 115 Stat. 272 (2001).

<sup>2</sup>Pub. L. No. 107-71, 115 Stat. 597 (2001).

<sup>3</sup>Pub. L. No. 107-295, 116 Stat. 2064 (2002).

stakeholder organizations that represent the broad spectrum of nonfederal governing entity interests in TSA's programs, such as the American Association of Port Authorities and the American Trucking Association to help identify nonfederal government entity credentialing programs and perspectives on TSA's credentialing programs.<sup>4</sup>

To determine how selected nonfederal governing entities' credentialing programs compare to TSA's programs, we analyzed pertinent federal laws, such as MTSA and the USA PATRIOT Act, and corresponding regulations related to the TWIC, HME, and Aviation Workers programs, as well as operational guidance and TSA policy documents for implementing the programs. By reviewing these laws, regulations, and policies, we identified requirements applicable to TSA and state and local governing agencies, as well as applicant eligibility standards such as lists of disqualifying criminal offenses and duration of time that agencies were required to consider these disqualifying criminal offenses ("look back period"). We then compared these standards and practices with those of identified programs that placed certain responsibilities upon nonfederal governing agency (state or local) programs we identified.

Through structured questions (in-person, phone, and email), we obtained information about credentialing programs and requirements in place by state and local governing agencies at selected maritime ports, airports, and state agencies. First, we collected information from maritime port authorities or other responsible nonfederal governing agencies at 17 maritime port locations—including the top 10 ports by container volume in 2010—plus 7 other ports we identified as having programs in place through information we obtained from industry groups, state agencies, and the U.S. Coast Guard. Collectively, the 17 maritime ports accounted for over 93 percent of U.S. waterborne foreign container trade in 2010, according to the U.S. Maritime Administration.<sup>5</sup> We visited officials at 5 of

---

<sup>4</sup>Other organizations we contacted included the Owner Operator Independent Drivers Association ; American Association of Motor Vehicle Administrators; American Association of Airport Executives; Institute of Makers of Explosives; National Petrochemical & Refiners Association; International Liquid Terminals Association; and Agricultural Retailers Association.

<sup>5</sup>The top 10 ports by container volume in 2010 were: Los Angeles, Calif.; Long Beach, Calif.; New York, N.Y.; Savannah, Ga.; Oakland, Calif.; Norfolk, Va.; Houston, Tex.; Seattle, Wash.; Charleston, S.C.; and Tacoma, Wash.. The additional seven ports we contacted include: Miami, Fla.; Port Everglades, Fla.; Baltimore, Md.; Wilmington, N.C.; Portland, Oreg.; Boston, Mass.; and Mobile, Ala.

these locations based on whether a state or local port authority had in place a credentialing program outside of TSA's TWIC program (Baltimore, Maryland; Norfolk, Virginia; Miami and Port Everglades, Florida; and New York, New York). Second, we collected information from 8 category X<sup>6</sup> airports including four of the top six airports by passenger boardings in 2009 plus 4 additional airports based on proximity to GAO locations.<sup>7</sup> The eight airports accounted for 23 percent of total U.S. domestic passenger boardings in 2009, according to the Federal Aviation Administration. We conducted site visits to three of these airports (Seattle-Tacoma International Airport, Washington Dulles International Airport, and Baltimore-Washington International Airport). Third, with respect to HME issuance, we collected information from six states, including the top five states as ranked by commercial drivers license issuance based on DOT data as of December 2010, plus one additional state that we identified as having additional requirements.<sup>8</sup> As of December 2010, the six states we contacted accounted for approximately one-third of the over 14 million commercial drivers licenses issued in the United States, according to information from DOT.<sup>9</sup> We visited officials at two state licensing agencies (New York State and Maryland). During our visits to maritime port facilities, state commercial drivers license issuing agencies, and airports, we interviewed officials, observed enrollment operations centers, and also reviewed cases of individuals who had been denied issuance of a state or local credential. Specifically, we obtained information from selected nonfederal government entities which included background check

---

<sup>6</sup>TSA classifies the nation's approximately 450 commercial airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings, and Category IV airports have the smallest.

<sup>7</sup>We obtained information from eight airports: Atlanta, Los Angeles; Denver; New York - JFK; Seattle-Tacoma International Airport; Washington-Dulles International Airport; Baltimore/Washington International; and Portland, Oregon.

<sup>8</sup>We obtained information from six states: California, Texas, Florida, New York, Illinois, Maryland.

<sup>9</sup>According to Department of Transportation officials, information on the number of HME endorsements by state was not available. Therefore, we used data provided by the department on the number of Master Pointer Records in the Commercial Driver's License Information System as a proxy for HME endorsements by state. The system is a database that contains certain information on individuals who have either been issued a commercial driver's license or who have been convicted of an offense in a vehicle that requires a commercial driver's license.

requirements as part of their credentialing programs. We obtained case information from these entities detailing denial of applicants' credentials. As part of this, we obtained case information from three ports with respect to individuals the port reported denying to or revoking local credentials from, because they had disqualifying criminal offenses based upon state program criteria. We provided information on 30 of these cases to TSA and then obtained case information on these 30 individuals from TSA—including whether TSA had identified these individuals as having potentially disqualifying criminal histories, whether they had obtained their TWIC through a waiver, and whether they had a valid TWIC as of July 1, 2011. While the information we obtained from nonfederal governing entity programs cannot be generalized across all states and localities, it provided us with a perspective on how state and local government transportation worker programs compare with federal programs and requirements.

To obtain information on challenges, if any, TSA faced in ensuring the effectiveness of its credentialing-related programs, we reviewed our prior reports related to the TWIC program and analyzed pertinent laws and regulations, including the National Crime Prevention and Privacy Compact Act of 1998.<sup>10</sup> We then analyzed TSA and FBI program documentation, including program training manuals, staffing plans, and other documents detailing program processes and challenges TSA faced, for the TWIC, HME, and Aviation Workers credentialing-related programs. In addition, we reviewed and compared TSA data detailing the number of enrollments and adjudication caseload for TSA's TWIC, HME, and Aviation Workers programs—covering the period of July 2010 through June 2011. Through interviews with knowledgeable TSA officials we determined that these data were sufficiently reliable for our purposes. To further obtain information on TSA credentialing-related practices and challenges, we interviewed headquarters officials from TSA's Transportation Threat Assessment and Credentialing (TTAC) program responsible for implementing the TWIC, HME, and Aviation Workers programs, DHS's Screening Coordination Office, responsible for coordinating credentialing programs across DHS; and the FBI's Criminal Justice Information Services Division, which maintains the FBI's national criminal history repository. We also visited the TTAC Adjudication Center in Herndon, Virginia to interview officials responsible for adjudicating TSA

---

<sup>10</sup>Pub. L. No. 105-251, 112 Stat. 1870, 1876 (1998) (codified at 42 U.S.C. 14616).

credentialing program applications and observe operations. We then evaluated the processes against TSA's credentialing program mission needs and *Standards for Internal Control in the Federal Government*.<sup>11</sup>

Additionally, we obtained the perspectives of nonfederal agency stakeholders, including officials from two organizations representing state criminal justice repository agencies—the National Crime Prevention and Privacy Compact Council<sup>12</sup> and SEARCH.<sup>13</sup> Collectively, these two organizations represent state criminal repository agencies from 50 states and the District of Columbia. The information we obtained through our interviews with nonfederal government entities and stakeholder organizations are not generalizable, but provided valuable perspectives related to TSA's TWIC, HME, and Aviation Workers programs.

We conducted this performance audit from February through November 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

<sup>11</sup>GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

<sup>12</sup>The Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and security of society while recognizing the importance of individual privacy rights.

<sup>13</sup>SEARCH is a nonprofit organization created by and for states which serves as the national consortium for justice information and statistics. It is governed by a Membership Group comprised of one gubernatorial appointee from each of the 50 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands, as well as eight at-large appointees selected by SEARCH's Chair. Members are primarily state-level justice officials responsible for operational decisions and policymaking concerning the management of criminal justice information, particularly criminal history information.

# Appendix II: TSA Credentialing Programs

TSA implements 17 credentialing programs which include conducting background checks—known as Security Threat Assessments—for a reported population of over 15 million individuals, such as those accessing airports, maritime ports, as well as for individuals seeking a hazardous material endorsement to their commercial driver’s license. The following table identifies and describes these programs.

**Table 3: TSA Credentialing Programs**

Program	Description
Airspace Waiver Program	TSA conducts a Security Threat Assessment on passengers and crew of flight operations into restricted U.S. airspace, flight operations into the U.S. for carriers that do not hold a TSA-approved security plan, and for all flight operations that transit US airspace without a takeoff or landing in the US (over flights) that do not hold a TSA-approved security plan.
Alien Flight Student Program	TSA conducts a Security Threat Assessment on foreign students seeking new or recurrent training at flight schools regulated by the Federal Aviation Administration (FAA).
Aviation Workers Program	Requires a Security Threat Assessment on individuals who apply for, or are issued personnel identification media at U.S. domestic airports, including airport facility workers, retail employees, and airline employees. TSA adjudicates terrorist and immigration checks, while airports adjudicate criminal history checks.
Certified Cargo Screening Program	Participation in this program is currently voluntary. As part of participation, TSA conducts a Security Threat Assessment on individuals who screen and work at a Certified Cargo Screening Facility.
DCA Access Standard Security Program	TSA conducts a Security Threat Assessment on all flight crewmembers (e.g. cockpit crew, flight attendants, cargo carrier employees) and passengers on non-commercial aircraft (non-cargo) flying into Ronald Reagan National Airport (DCA) from 1 of 22 domestic gateway airports or out of DCA
FAA Airmen Certificate Program	TSA conducts a Security Threat Assessment on all FAA Airmen Certificate holders and applicants for a certificate based on a foreign license.
Full All Cargo Security Program	TSA conducts a Security Threat Assessment on certain individuals with unescorted access to air cargo for each operation that is in an aircraft with a maximum certification takeoff weight of more than 45,500 kg (100,309.3 pounds) and carrying cargo and authorized persons and no passengers.
Hazardous Materials Endorsement Threat Assessment Program	TSA conducts a Security Threat Assessment on drivers wishing to obtain a hazardous materials endorsement on a state-issued commercial driver’s license.
Indirect Air Carrier Program	TSA conducts a Security Threat Assessment on individuals who perform screening, supervise screening, or have unescorted access to air cargo bound for commercial airlines, as well as qualified shippers and certain individuals in managerial or ownership roles of an indirect air carrier.
Maryland Three Program	TSA conducts a Security Threat Assessment on pilots who operate aircraft and apply for privileges to fly to or from the three General Aviation airports in the Washington, D.C. restricted flight zones (Potomac Airport, Washington Executive/Hyde Field, and College Park Airport).



**Appendix II: TSA Credentialing Programs**

<b>Program</b>	<b>Description</b>
Merchant Mariner Credential	TSA and Coast Guard conduct a Security Threat Assessment and safety and suitability check on individuals seeking employment aboard U.S. merchant vessels greater than 100 Gross Register Tons (Domestic Tonnage), except operators of uninspected passenger vessels
Private Charter Standard Security Program	TSA conducts a Security Threat Assessment on private charter flight crewmembers operating aircraft with a maximum certificated takeoff weight of 45,500kg (100,309 pounds) or more, or a passenger-seating configuration of 61 or more, or whose passengers are enplaned from or deplaned into a sterile area.
SSI / Civil Litigant Program	TSA conducts a Security Threat Assessment on individuals who seek access to Sensitive Security Information in the course of civil litigation.
Secure Flight	TSA conducts uniform prescreening of passenger information against federal government watch lists for all domestic and international passengers traveling on covered flights into, out of, within, or over the United States.
Master Crew Vetting Program	TSA conducts a Security Threat Assessment on flight crewmembers entering, departing, or flying over U.S. airspace.
Transportation Worker Identification Credential	TSA conducts a Security Threat Assessment on individuals who require unescorted access to secure areas of regulated maritime facilities, vessels, and all merchant mariners.
Twelve - Five Standard Security Program	TSA conducts a Security Threat Assessment on flight crewmembers operating aircraft with a maximum certificated takeoff weight of 12,500 pounds or more.

Source: GAO analysis of TSA information.

# Appendix III: TSA TWIC, HME, and Aviation Workers Programs: Legislative Background and Purpose

Following September 11 2001, legislation was enacted into law that was designed to ensure that transportation workers, particularly those who transport hazardous materials or require unescorted access to secure areas of federally regulated maritime or airport transportation facilities are properly vetted to identify whether they pose a security threat. In response, TSA established the TWIC, HME, and Aviation Workers programs. The following summarizes the legislative background and purpose of these three programs.

**Table 4: Legislative Background and Purpose of TSA’s TWIC, HME, and Aviation Workers Programs**

Program	Legislative Background and Purpose
TWIC	<p>In November 2001, the Aviation and Transportation Security Act (ATSA)<sup>a</sup> was enacted, requiring TSA to, among other things, work with airport operators to strengthen access control points to secured areas and to consider using biometric access control systems, or similar technologies, to verify the identity of individuals who seek to enter a secure airport area. In response to ATSA, TSA established the TWIC Program in December 2001. The Maritime Transportation Security Act of 2002 (MTSA)<sup>b</sup> required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they possess a biometric transportation security card and are authorized to be in such an area. MTSA further tasked the Secretary with the responsibility to issue biometric transportation security cards to eligible individuals unless the Secretary determines that an applicant poses a security risk warranting denial of the card. The TWIC Program is designed to implement these biometric maritime security card requirements—with TSA responsible for conducting Security Threat Assessments and MTSA-regulated port facilities—including private facilities and public port authorities—responsible for verifying that workers have a valid TWIC and a valid business case to access their facility. TSA has issued and activated over 1.7 million TWICs to maritime port workers and denied 1,332 applications as of June 2011.<sup>c</sup></p>
HME	<p>The USA PATRIOT Act of 2001<sup>d</sup> prohibits states from issuing a motor vehicle license to individuals seeking to transport hazardous materials in commerce unless a determination has been made by the Secretary of Transportation that the individual does not pose a security risk warranting denial of the license. TSA developed regulations to implement this requirement,<sup>e</sup> and TSA established the HME Program in order to conduct Security Threat Assessments for truckers seeking to obtain, renew, or transfer a HME on their state-issued commercial driver’s license. The Federal Motor Carrier Safety Administration within DOT oversees license issuance policy and issued a companion rule indicating that state motor vehicle agencies can not issue a HME until the applicant has first met TSA vetting standards. State motor vehicle agencies are responsible for ensuring that TSA has vetted these applicants before it issues a HME. As of June 2011, TSA reported conducting Security Threat Assessments on approximately 1.5 million HME applicants, and denying over 15,000 applications.</p>

**Appendix III: TSA TWIC, HME, and Aviation Workers Programs: Legislative Background and Purpose**

<b>Program</b>	<b>Legislative Background and Purpose</b>
Aviation Workers Program	<p>ATSA established TSA within DOT as the federal agency responsible for civil aviation security responsibilities.<sup>f</sup> Pursuant to ATSA, responsibility for the security of civil aviation was transferred from the Federal Aviation Administration to TSA, along with the Federal Aviation Administration's existing aviation security programs, plans, regulations, orders, and directives. Among other things, ATSA directs TSA to improve the security of airport perimeters and the access controls leading to secured areas, and take measures to reduce the security risks posed by airport workers. TSA corresponding regulations require that before airport and aircraft operators issue identification media to workers seeking unescorted access authority to sterile areas or a Security Identification Display Area (SIDA), they must undergo a fingerprint-based criminal history record check. TSA subsequently issued a Security Directive requiring that airport operators may not issue identification media to individuals who work in or have access to the Air Operations Area unless they undergo a Security Threat Assessment including name based terrorism and immigration status checks.<sup>g</sup> TSA reports that approximately 1.2 million workers currently hold airport badges.</p>

Source: GAO analysis of DHS information

Notes:

<sup>a</sup>Pub. L. No. 107-71, 115 Stat. 597, 610 (2001).

<sup>b</sup>Pub. L. No. 107-295, 116 Stat. 2064, 2073-74 (2002).

<sup>c</sup>The number of denials refers specifically to the number of final disqualification letters issued by TSA. Some denial letters could be repeat applicants. TSA also has waiver and appeals processes, so the number of initial disqualification letters issued is greater—over 90,000, according to TSA.

<sup>d</sup>Pub.L. No.107-56, 115 Stat. 272, 396-97 (2001).

<sup>e</sup>49 C.F.R. Part 1572.

<sup>f</sup>TSA was subsequently transferred from DOT to DHS in March 2003. See Pub. L. No. 107-296, § 403(2), 116 Stat. 2135, 2178 (2002).

<sup>g</sup>SD 1542-04-08G.

---

# Appendix IV: Criminal Offenses That May Disqualify Applicants from Acquiring a TWIC or HME

---

Listed below are criminal offenses that can prevent TWIC or HME applicants from being issued a credential. Pursuant to TSA implementing regulations, permanent disqualifying criminal offenses are those offenses listed in 49 C.F.R. § 1572.103(a) for which an applicant has a felony conviction, or has been found not guilty by reason of insanity, in a civilian or military jurisdiction. Interim disqualifying criminal offenses are those offenses listed in 49 C.F.R. § 1572.103(b) for which the applicant has either (1) a felony conviction, or been found not guilty by reason of insanity, within a 7-year period preceding the application, or (2) incarcerated for that crime within a 5-year period preceding the application. Applicants with certain permanent disqualifying criminal offenses and all interim disqualifying criminal offenses may request a waiver of their disqualification pursuant to 49 C.F.R. § 1515.7. In general, TSA may issue such a waiver and grant a TWIC or HME if TSA determines that an applicant does not pose a security threat based upon the Security Threat Assessment.

**Permanent disqualifying criminal offenses for which no waiver may be granted.**

1. Espionage, or conspiracy to commit espionage.
2. Sedition, or conspiracy to commit sedition.
3. Treason, or conspiracy to commit treason.

A federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable State law, or conspiracy to commit such crime.

**Permanent disqualifying criminal offenses for which a waiver may be granted.**

1. A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. § 70101. The term 'economic disruption' does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.
2. Improper transportation of a hazardous material under 49 U.S.C. § 5124, or a State law that is comparable.

3. Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. §§ 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. § 921(a)(4) and 26 U.S.C. § 5845(f).
4. Murder.
5. Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility.
6. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961, et seq., or a comparable State law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph 49 C.F.R. § 1572.103 (a).
7. Attempt to commit the crimes in paragraphs listed under 49 C.F.R. § 1572.103 (a)(1) through (a)(4).
8. Conspiracy or attempt to commit the crimes in 49 C.F.R. § 1572.103 (a)(5) through (a)(10).

**Interim disqualifying criminal offenses.**

1. Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. § 921(a)(3) or 26 U.S.C. § 5845(a), or items contained on the United States Munitions Import List at 27 C.F.R. § 447.21.
2. Extortion.
3. Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in 49 C.F.R. § 1572.103 (a) or (b). Welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.

---

**Appendix IV: Criminal Offenses That May  
Disqualify Applicants from Acquiring a TWIC  
or HME**

---

4. Bribery.
5. Smuggling.
6. Immigration violations.
7. Distribution of, possession with intent to distribute, or importation of a controlled substance.
8. Arson.
9. Kidnapping or hostage taking.
10. Rape or aggravated sexual abuse.
11. Assault with intent to kill.
12. Robbery.
13. Fraudulent entry into a seaport as described in 18 U.S.C. § 1036, or a comparable State law.
14. Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961, et seq., or a comparable State law, other than the violations listed in paragraph 49 C.F.R. § 1572.103 (a)(10).
15. Conspiracy or attempt to commit the interim disqualifying criminal offenses.

---

# Appendix V: Criminal Offenses That Disqualify Applicants under the Aviation Workers Program from Acquiring an Airport-Issued Access Badge

---

Listed below are the disqualifying criminal offenses that, in general, prevent individuals under the Aviation Workers Program seeking unescorted access to secure areas of an airport from being issued an airport access credential. Pursuant to 49 C.F.R. §§1542.209, 1544.229, 1544.230, and Security Directive 1542-04-08G, an individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the crimes listed below in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority. In contrast to TWIC and HME, there is no waiver process for any of the disqualifying criminal offenses. However, none of the crimes are permanently disqualifying—disqualifying criminal offenses are those specified offenses for which an individual has been convicted, or found not guilty by reason of insanity during the 10 years before the date of the individual's application. As such, we refer to them below as interim disqualifying criminal offenses for which no waiver may be granted.

**Interim disqualifying criminal offenses for which no waiver may be granted.**

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. § 46306.
2. Interference with air navigation; 49 U.S.C. § 46308.
3. Improper transportation of a hazardous material; 49 U.S.C. § 46312.
4. Aircraft piracy; 49 U.S.C. § 46502.
5. Interference with flight crew members or flight attendants; 49 U.S.C. § 46504.
6. Commission of certain crimes aboard aircraft in flight; 49 U.S.C. § 46506.
7. Carrying a weapon or explosive aboard aircraft; 49 U.S.C. § 46505.
8. Conveying false information and threats; 49 U.S.C. § 46507.
9. Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. § 46502(b).

---

**Appendix V: Criminal Offenses That Disqualify Applicants under the Aviation Workers Program from Acquiring an Airport-Issued Access Badge**

---

10. Lighting violations involving transporting controlled substances; 49 U.S.C. § 46315.
11. Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. § 46314.
12. Destruction of an aircraft or aircraft facility; 18 U.S.C. § 32.
13. Murder.
14. Assault with intent to murder.
15. Espionage.
16. Sedition.
17. Kidnapping or hostage taking.
18. Treason.
19. Rape or aggravated sexual abuse.
20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
21. Extortion.
22. Armed or felony unarmed robbery.
23. Distribution of, or intent to distribute, a controlled substance.
24. Felony arson.
25. Felony involving a threat.
26. Felony involving—
  - (i) Willful destruction of property;
  - (ii) Importation or manufacture of a controlled substance;
  - (iii) Burglary;
  - (iv) Theft;



---

**Appendix V: Criminal Offenses That Disqualify Applicants under the Aviation Workers Program from Acquiring an Airport-Issued Access Badge**

---

- (v) Dishonesty, fraud, or misrepresentation;
- (vi) Possession or distribution of stolen property;
- (vii) Aggravated assault;
- (viii) Bribery; or
- (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

27. Violence at international airports; 18 U.S.C. § 37.

28. Conspiracy or attempt to commit any of the criminal acts listed above.

# Appendix VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

November 30, 2011

Mr. Stephen M. Lord  
Director, Homeland Security and Justice Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Re: Draft Report GAO-12-60, "TRANSPORTATION SECURITY: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload"

Dear Mr. Lord:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Transportation Security Administration (TSA) employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our Nation's transportation system. TSA also works closely with other federal agencies and maximizes participation from state, local, tribal, and private-sector stakeholders to develop a common goal of securing all modes of transportation, including aviation, maritime, and surface transportation.

As part of its operations, TSA conducts security threat assessments (STAs) to determine whether an applicant seeking access to critical components of the Nation's transportation system poses or is suspected of posing a threat to transportation or national security. An STA may differ from mode-to-mode or program-to-program based on statutory, policy, or resource requirements at the time of program implementation. An STA includes any combination of fingerprint-based criminal history records check, a lawful presence check, and checks for ties to terrorism.

TSA's vetting responsibilities have grown significantly in recent years. TSA has responded with the development and implementation of efficient, reliable, and cost-effective terrorist-related screening programs. TSA perpetually vets more than 14 million records per day, adjudicates more than 12,000 cases per week, and responds to more than 400 redress requests per week.

GAO's report focused on three TSA STA programs. Specifically, the:

1. Aviation Workers Program, which covers individuals—including airport facility workers, retail employees, and some airline employees—who apply for, or are issued,

personnel identification media at U.S. domestic airports. The current active badged population is approximately 2.1 million, with approximately 450,000 new applicants per year.

2. Transportation Worker Identification Credential Program, which covers individuals who must access secure areas of maritime facilities, ports, and vessels, and merchant mariners. In the last 4 years, more than 2 million workers have enrolled in the TWIC program. TSA has processed 50,000 appeals and waiver requests.
3. Hazardous Materials Endorsement Program, which covers drivers seeking to obtain, renew, or transfer an HME on a state-issued commercial driver's license. This endorsement is required to haul any material that requires placarding under the U.S. Department of Transportation hazardous materials regulations. Since the HME program inception in 2005, more than 1.8 million individuals have applied for a new or renewed HME STA.

DHS recognizes that there are criminal records at the state level, which TSA does not receive. There are two primary reasons for this. First, the states do not always upload all their criminal records to the Federal Bureau of Investigation (FBI) biometric criminal recordation system. Second, states do not respond to criminal history record information (CHRI) requests for "non-criminal justice purposes,"<sup>1</sup> and the states and U.S. Department of Justice (DOJ) currently view TSA's transportation worker vetting programs as "non-criminal justice" activities. In addition, because of this designation, TSA is unable to request subsequent CHRI for recurrent vetting without a submission of new fingerprints and fees from the individual. TSA's level of CHRI access is equal to that of a private company doing an employment check on a new applicant.

To provide the most robust vetting against criminal history records so that TSA can effectively meet its statutory requirements to mitigate risks to the security of the Nation's transportation systems, TSA should have full access to CHRI. DHS, in coordination with TSA, will continue to work with DOJ, the FBI, and the states to expand access to the CHRI.

The draft report contained three recommendations with which DHS concurs and has already initiated steps to implement. Specifically, GAO recommended that:

**Recommendation 1:** The Secretary of Homeland Security and the Attorney General of the United States jointly assess the extent to which a security risk may exist with respect to the level of access to criminal history records information currently received by TSA to complete STAs, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative.

<sup>1</sup> "Non-criminal justice purposes" means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. (42 U.S.C. § 14616)

**Response:** Concur. DHS looks forward to working with DOJ to assess the extent of security risk, identify alternatives to address any risks, and evaluate the costs and benefits of each alternative. As you know, TSA has been working with DOJ, the FBI, and states for several years to obtain more comprehensive access to CHRI. We have explored the possibility that DOJ view TSA's transportation worker vetting as "criminal justice" purposes<sup>2</sup> (to which all 50 states and the District of Columbia respond); designate TSA's transportation vetting as a "national security" purpose (to which 45 states currently respond); or use current statutory and regulatory authority<sup>3</sup> to provide more access to criminal records.

As of mid-October 2011, TSA and the FBI implemented a pilot program to use the FBI Interstate Identification Index (III) to obtain state CHRI along with the FBI's CHRI in an automated fashion. TSA currently receives automated data from 14 states, and the pilot program will provide information from 22 additional states that respond to non-criminal justice requests through the III. The solution involves querying III for additional state-level information if the FBI CHRI contains any information from the state for a given individual. DHS and the FBI have also begun discussions regarding another pilot project to address recurrent criminal history inquiries, also known as "rapback." The FBI has proposed piloting an interim or manual rapback solution with TSA for spring/summer 2012 before its automated rapback capability (targeted for 2014–2015) occurs.

The III check and rapback pilot projects will be implemented for those individuals who have criminal records in the FBI database when the STA is first conducted. The projects will identify individuals who have a previous criminal history with the FBI at the start of the STA process. Thus, TSA will not receive records for: 1) individuals who have criminal history records at the state level only; or 2) individuals with no initial criminal records but who commit criminal offenses after the STA is approved.

As the pilots progress, TSA will work with the FBI to identify the differences between the standard FBI CHRI non-criminal justice results and the additional state data. TSA will work with the FBI to include these results in the overall assessment of risks regarding TSA's current level of CHRI access.

**Recommendation 2:** The Secretary of Homeland Security direct the TSA Administrator to conduct an assessment of the risks associated with not utilizing some state-provided criminal history information, as well as an analysis of the costs and benefits of integrating the information into the current adjudication process.

**Response:** Concur. Although TSA does not believe it needs to conduct an assessment of the risk or cost and benefit analysis, TSA concurs with the intent of this recommendation and, as described in Recommendation 1, has already identified a solution that can be discussed.

<sup>2</sup> "Criminal justice" includes activities relating to the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history records. (42 U.S.C. § 14616)

<sup>3</sup> See 28 U.S.C. § 534; 28 CFR § 20.33(a) (2).

Since 2005, TSA has conducted assessments to identify alternatives to integrate state-level data. TSA worked with the states, FBI, and the National Crime Prevention and Privacy Compact Council to convene working groups to identify possible solutions to receive data directly from other states and a standard, automated, more cost-efficient and effective solution. TSA later leveraged these efforts in the TWIC program and other STA programs that require criminal history records checks. TSA discovered multiple problems with obtaining information directly from the states:

1. The states have varying data systems and legal and practical constraints, and TSA would likely be required to develop and build a unique solution for each state to request data directly from all states for each STA case. To minimize these problems, TSA has discussed with the states an option of defining one common technical solution through which states could send their data directly to TSA. TSA is pursuing this as part of the Transportation Threat Assessment and Credentialing (TTAC) Infrastructure Modernization program, which was established to standardize and consolidate TSA's security threat assessment systems.
2. Because many transportation workers have resided in and continually travel across multiple states, requesting and receiving state-level data from only an applicant's state of residence or enrollment is inadequate and may miss criminal history in other states.
3. Some states may require additional fees to respond to TSA's request directly, rather than using the FBI's system. As required by statute, TSA's transportation worker vetting programs are funded through user fees; this additional cost could dramatically increase fees to the workers.

For the listed reasons, TSA has determined that using the established FBI III system to request and receive data from all states would be the most effective and efficient solution. State criminal history data may be accessed via the III system managed by the FBI. The extent of access to state data is based on the purpose of the data request. Currently, a request must be deemed a "criminal justice" purpose to receive the full breadth of CHRI available from all 50 states and the District of Columbia. Many states may not upload all available information into the FBI biometric system made available to TSA today, and many states do not provide their III records for non-criminal justice activities. If the pilot with the FBI is successful, this method of using the state information may prove to be the most efficient and effective means of sharing the most complete CHRI.

**Recommendation 3:** The Secretary of Homeland Security direct the TSA Administrator to develop a workforce staffing plan with timelines articulating how the TTAC Adjudication Center will effectively and efficiently meet its current and emerging workload requirements, and incorporate the results of TSA's study examining the appropriateness and costs and benefits of using contractors.

**Response:** Concur. Although TSA does not believe that the TTAC Adjudication Center has challenges in meeting its workload requirements, we concur with the recommendation and have

been working on these strategies since before issuance of this draft report. TSA is currently meeting its Adjudication Center workload requirements and provided GAO a copy of the workforce staffing plan. TSA recognizes the importance of appropriately balancing its federal and contractor workforce and, in 2010, began a review to ensure that the right workforce balance is achieved. TSA is analyzing the results of this review to achieve the best balance of federal and contractor resources as part of the Department-wide Balanced Workforce Strategy. The results will be available once finalized.

As new STA programs are legislated and defined in regulation, TSA will continue to assess the staffing needs to implement each emerging STA requirement on the basis of Balanced Workforce Strategy results.

Again, thank you for the opportunity to review and comment on this draft report. Sensitivity comments were previously provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker  
Director  
Departmental GAO-OIG Liaison Office

---

# Appendix VII: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Stephen M. Lord at (202) 512-4379 or [lords@gao.gov](mailto:lords@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, David Bruno, Assistant Director, and Jason Berman, Analyst-in-Charge, managed this assignment. David Bieler, James Lawson, and Rebecca Kuhlmann Taylor made significant contributions to this report. Michele Fejfar and Richard Hung assisted with design and methodology. Geoffrey Hamilton provided legal support. Tina Cheng, Jessica Orr, and Robert Robinson provided assistance in report preparation.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

