United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2011

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives

GAO-11-657

May 2011

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives

GAO Highlights

Accountability • Integrity • Reliability

Highlights of GAO-11-657, a report to congressional requesters

Why GAO Did This Study

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program, which requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities. As requested, GAO evaluated the extent to which (1) TWIC processes for enrollment, background checking, and use are designed to provide reasonable assurance that unescorted access to these facilities is limited to qualified individuals; and (2) the effectiveness of TWIC has been assessed. GAO reviewed program documentation, such as the concept of operations, and conducted site visits to four TWIC centers, conducted covert tests at several selected U.S. ports chosen for their size in terms of cargo volume, and interviewed agency officials. The results of these visits and tests are not generalizable but provide insights and perspective about the TWIC program. This is a public version of a sensitive report. Information DHS deemed sensitive has been redacted.

What GAO Recommends

Among other things, GAO recommends that DHS assess TWIC program internal controls to identify needed corrective actions, assess TWIC's effectiveness, and use the information to identify effective and cost-efficient methods for meeting program objectives. DHS concurred with all of the recommendations.

View GAO-11-657 or key components. For more information, contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

Internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of Maritime Transportation Security Act (MTSA)-regulated facilities is restricted to qualified individuals. To meet the stated program purpose, TSA designed TWIC program processes to facilitate the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls designed and in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. GAO found that internal controls in the enrollment and background checking processes are not designed to provide reasonable assurance that (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC-holders have maintained their eligibility. Further, internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of MTSA-regulated facilities during covert tests conducted by GAO's investigators. During covert tests of TWIC use at several selected ports, GAO's investigators were successful in accessing ports using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (i.e., reasons for requesting access). Conducting a control assessment of the TWIC program's processes to address existing weaknesses could better position DHS to achieve its objectives in controlling unescorted access to the secure areas of MTSA-regulated facilities and vessels.

DHS has not assessed the TWIC program's effectiveness at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned, is more effective than prior approaches used to limit access to ports and facilities, such as using facility specific identity credentials with business cases. Conducting an effectiveness assessment that further identifies and assesses TWIC program security risks and benefits could better position DHS and policymakers to determine the impact of TWIC on enhancing maritime security. Further, DHS did not conduct a risk-informed cost-benefit analysis that considered existing security risks, and it has not yet completed a regulatory analysis for the upcoming rule on using TWIC with card readers. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program, could help DHS ensure that the TWIC program is more effective and cost-efficient than existing measures or alternatives at enhancing maritime security.

Contents

Tables

Figure

Abbreviations

ATSA	Aviation and Transportation Security Act
CSOC	Colorado Springs Operations Center
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
IAFIS	Integrated Automated Fingerprint Identification System
III	Interstate Identification Index
MISLE	Marine Information for Safety and Law Enforcement
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act
NCIC	National Crime Information Center
NIPP	National Infrastructure Protection Plan
SAFE Port Act	Security and Accountability For Every Port Act
SAVE	Systematic Alien Verification for Entitlements
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 10, 2011

Congressional Requesters

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 United States economy and necessary for supporting international commerce. As we have previously reported, these systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.[1]

The Maritime Transportation Security Act of 2002[2] (MTSA) 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.[3] 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 Transportation Worker Identification Credential (TWIC) program is designed to implement these biometric maritime security card requirements. The program requires maritime workers to complete background checks to obtain a biometric identification card and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and

[1]See GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009); *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sept. 29, 2006); and *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: Dec. 10, 2004).

[2]Pub. L. No. 107-295, 116 Stat. 2064 (2002).

[3]Under Coast Guard 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.

vessels.[4] According to the Coast Guard, as of December 2010 and January 2011, there were 2,509 facilities and 12,908 vessels, respectively, which are subject to MTSA regulations and must implement TWIC provisions.[5]

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard are responsible for implementing and enforcing the TWIC program. TSA's responsibilities include enrolling TWIC applicants, conducting background checks to assess the individual's security threat, and issuing TWICs. 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 addition, DHS's Screening Coordination Office facilitates coordination among the various DHS components involved in TWIC, such as TSA and the Coast Guard, as well as the U.S. Citizenship and Immigration Services, which personalizes the credentials,[6] and the Federal Emergency Management Agency, which administers grant funds in support of the TWIC program.

In January 2007, a federal regulation (known as the TWIC credential rule) set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker seeking unescorted access to secure areas of MTSA-regulated facilities and vessels must possess a TWIC.[7] In September 2008, we reported that TSA, the Coast Guard, and maritime industry stakeholders (e.g., operators of MTSA-regulated facilities and vessels) had faced challenges in implementing the TWIC program, including enrolling and issuing TWICs to a larger population than was originally anticipated, ensuring that TWIC access control technologies perform effectively in the harsh maritime environment, and balancing

[4] 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.

[5] 33 C.F.R. Part 105, for example, governs maritime facility security and sets forth general security requirements along with requirements for facility security assessments and facility security plans, among other things. General maritime security requirements pertaining to vessels are set out in 33 C.F.R. Part 104.

[6] A card is personalized when the card holder's personal information, such as photograph and name, are added to the card.

[7] 72 Fed. Reg. 3492 (2007); Extension of deadline to April 15, 2009 by 73 Fed. Reg. 25562 (2008).

security requirements with the flow of maritime commerce.[8] In November 2009, we reported that progress had been made in enrolling workers and activating TWICs, and recommended that TSA develop an evaluation plan to guide pilot efforts and help inform the future implementation of TWIC with electronic card readers.[9] DHS generally concurred and discussed actions to implement the recommendations, but these actions have not yet fully addressed the intent of all of the recommendations. Currently, TWICs are primarily used as visual identity cards—known as a flashpass—where a card is to be visually inspected before a cardholder is allowed unescorted access to a secure area of a MTSA-regulated port or facility.[10] As of January 6, 2011, TSA reported over 1.7 million enrollments and 1.6 million cards issued and activated.[11]

In response to your request, we evaluated the extent to which TWIC program controls provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to those possessing a legitimately issued TWIC and who are authorized to be in such an area. Specifically, this report addresses the following questions:

1. To what extent are TWIC processes for enrollment, background checking, and use designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals?
2. To what extent has DHS assessed the effectiveness of TWIC, and does the Coast Guard have effective systems in place to measure compliance?

This report is a public version of a related sensitive report that we issued to you in May 2011. DHS and TSA deemed some of the information in the prior report as sensitive security information, which must be protected from public disclosure. Therefore, this report omits sensitive information

[8] GAO, *Transportation Worker Identification Credential: A Status Update*, GAO-08-1151T (Washington, D.C.: Sept. 17, 2008).

[9] GAO-10-43.

[10] TWIC guidance provides that possession of a TWIC is required for an individual to be eligible for unescorted access to secure areas of vessels and facilities. With the issuance of a TWIC, it is still the responsibility of facility and vessel owners to determine who should be granted access to their facilities or vessels.

[11] Prior to issuing a TWIC, each TWIC is activated, or turned on, after the person being issued the TWIC provides a personal identification number.

about the TWIC program, including techniques used to enroll and conduct a background check on individuals and assess an individual's eligibility for a TWIC, and the technologies that support TWIC security threat assessment determinations and Coast Guard inspections. In addition, at TSA's request, we have redacted data on specific enrollment center(s) and maritime ports where our investigators conducted covert testing. Although the information provided in this report is more limited in scope, it addresses the same questions and includes the same recommendations as the sensitive report. Also, the overall methodology used for both reports is the same.

To assess the extent to which TWIC program processes were designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals, we reviewed applicable laws, regulations, and policies.[12] We also reviewed documentation provided by TSA on the TWIC program systems and processes, such as the TWIC User Manual for Trusted Agents, Statement of Objectives, and Concept of Operations. We further reviewed the processes and data sources with TWIC program management from TSA and Lockheed Martin (the contractor responsible for implementing the program).[13] We also met with (1) the Director of Vetting Operations at TSA's Colorado Springs Operations Center (CSOC), where background checks for links to terrorism and continual vetting of TWIC holders is to take place; (2) the Operations Manager for the Adjudication Center, where secondary background checks are to be conducted for applicants with identified criminal or immigration issues; and (3) the Director at DHS's Screening Coordination Office responsible for overseeing credentialing

[12] See, for example, MTSA, Security and Accountability For Every Port Act (SAFE Port Act) of 2006 (Pub. L. No. 109-347, 120 Stat. 1884 (2006)) amendments to MTSA, Navigation and Vessel Inspection Circular Number 03-07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, D.C.: July 2, 2007), Coast Guard Policy Advisory Council (PAC) decisions, and Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[13] To assess the reliability of data on the number of TWIC enrollments, the number of self-identified U.S. citizens or nationals asserting themselves to be born in the United States or in a U.S. territory, and the number of TWICs approved after the initial background check, we reviewed program systems documentation and interviewed knowledgeable agency officials about the source of the data and the controls the TWIC program and systems had in place to maintain the integrity of the data. We determined that the data were sufficiently reliable for the purposes of our report. The data we reviewed were collected between October 2007 and December 2010.

programs across DHS. Additionally, we met with the Criminal Justice Information Services Division at the Federal Bureau of Investigation (FBI) to discuss criminal vetting processes and policies. We then evaluated the processes against the TWIC program's mission needs and *Standards for Internal Control in the Federal Government*.[14] As part of our assessment of TWIC program controls, we also did the following.

- We visited four TWIC enrollment and activation centers located in areas with high population density and near ports participating in the TWIC pilot to observe how TWIC enrollments are conducted.[15] The results are not generalizable to all enrollment and activation centers; however, because all centers are to conduct the same operations following the same guidance, the locations we visited provided us with an overview of the TWIC enrollment and activation/issuance processes.

- We had our investigators conduct covert testing at enrollment center(s) operating at the time to identify whether individuals providing fraudulent information could acquire an authentic TWIC. The information we obtained from the covert testing at enrollment center(s) is not generalizable across all TWIC enrollment centers. However, because all enrollments are to be conducted following the same established processes, we believe that the information from our covert tests provided us with important perspective on TWIC program enrollment and background checking processes, as well as potential challenges in verifying an individual's identity.

Further our investigators conducted covert testing at several selected maritime ports with MTSA-regulated facilities and vessels to identify security vulnerabilities and program control deficiencies. These locations were selected based on their geographic location across the country (east coast, gulf coast, and west coast) and port size in terms of cargo volume. We also visited or met with officials at each of the seven original pilot sites

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

[15] We visited the Howland Hook enrollment center in Staten Island, New York, the Whitehall Ferry Terminal enrollment center in New York, New York, the Terminal Island enrollment center in San Pedro, California, and the Long Beach enrollment center in Long Beach, California.

being used to test TWIC card readers,[16] interviewed port security officials at two additional ports responsible for implementing TWIC at their port,[17] and met with nine maritime or transportation industry associations[18] to obtain information on (1) the use of TWIC as a flashpass and with biometric readers where they are in use, (2) experiences with TWIC card performance, and (3) any suspected or reported cases of TWIC card fraud. The information we obtained from the security officials at the 9 ports or pilot participants we visited is not generalizable across the maritime transportation industry as a whole, but collectively, the ports we visited accounted for 56 percent of maritime container trade in the United States, and the ports our investigators visited as part of our covert testing efforts accounted for 54 percent of maritime container trade in the United States in 2009. As such, we believe that the information from these interviews, site visits, and covert tests provided us with important additional perspective and context on the TWIC program, as well as information about potential implementation challenges faced by MTSA-regulated facilities/vessels, transportation workers, and mariners.

To assess the extent to which DHS has assessed the effectiveness of TWIC, and determine whether the Coast Guard has effective systems in place to measure compliance, we reviewed applicable laws, regulations,

[16] We visited pilot participants at the Ports of Los Angeles, Long Beach, and Brownsville, and the Port Authority of New York and New Jersey. We also interviewed and or met with officials at vessel operations participating in the TWIC pilot, including the Staten Island Ferry in Staten Island, New York; Magnolia Marine Transports in Vicksburg, Mississippi; and Watermark Cruises in Annapolis, Maryland.

[17] We met with officials responsible for implementing TWIC at the Port of Baltimore and the Port of Houston. We selected the Port of Baltimore based on proximity to large population centers and we selected the Port of Houston because it was using TWICs with readers.

[18] We interviewed representatives from the Association of the Bi-State Motor Carriers, the New Jersey Motor Truck Association, the Association of American Railroads, the American Public Transportation Association, the American Association of Port Authorities, the International Liquid Terminals Association, the International Longshore and Warehouse Union, the National Employment Law Project, and the Passenger Vessel Association. These organizations were selected because together they represent the key constituents of port operations.

and policies.[19] We also met with TWIC program officials from TSA and the Coast Guard, as well as Coast Guard officials responsible for assessing maritime security risk, and reviewed related documents, to identify how TWIC is to enhance maritime security.[20] In addition, we met with Coast Guard TWIC program officials, data management staff, and Coast Guard officials stationed at four port areas across the United States with enforcement responsibilities to assess the agency's approach to enforcing compliance with TWIC regulations and measuring program effectiveness.[21] As part of this effort, we reviewed the type and substance of management information available to the Coast Guard for assessing compliance with TWIC. In performing this work, we evaluated the Coast Guard's practices against TWIC program mission needs and *Standards for Internal Control in the Federal Government.*

We conducted this performance audit from November 2009 through March 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. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.[22]

[19] See, for example, MTSA, Security and Accountability For Every Port Act (SAFE Port Act) of 2006 (Pub. L. No. 109-347, 120 Stat. 1884 (2006)) amendments to MTSA, Navigation and Vessel Inspection Circular Number 03-07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, D.C.: July 2, 2007), Coast Guard Policy Advisory Council (PAC) decisions, and Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[20] See, for example, the Coast Guard's 2008 Analysis of Transportation Worker Identification Credential (TWIC) Electronic Reader Requirements in the Maritime Sector, and the Homeland Security Institute's 2008 Independent Verification and Validation of Development of Transportation Worker Identification Credential (TWIC) Reader Requirements.

[21] We interviewed Coast Guard officials in New York and New Jersey; Los Angeles and Long Beach, California; Corpus Christi, Texas; and Baltimore, Maryland. We met with these Coast Guard officials because the facilities, vessels, and enrollment centers we visited are housed in these officials' area(s) of responsibility.

[22] During the course of the audit, we provided briefings on the preliminary results of our work in May and October 2010.

Background

TWIC History and Purpose

In November 2001, the Aviation and Transportation Security Act (ATSA)[23] 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.[24] In November 2002, MTSA was enacted and required the Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics to control access to secure areas of maritime transportation facilities and vessels.[25] In addition, the Security and Accountability For Every Port Act (SAFE Port Act) of 2006 amended MTSA and directed the Secretary of Homeland Security to, among other things, implement the TWIC pilot project to test TWIC use with biometric card readers and inform a future regulation on the use of TWIC with electronic readers.

In requiring the issuance of transportation security cards for entry into secure areas of a facility or vessel as part of MTSA, Congress noted in the "Findings" section of the legislation that ports in the United States are a major location for federal crime such as cargo theft and smuggling, and are susceptible to large-scale acts of terrorism.[26] For example, according to the Coast Guard's January 2008 National Maritime Terrorism Threat Assessment, al Qaeda leaders and supporters have identified western maritime assets as legitimate targets.[27] Moreover, according to the Coast

[23] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[24] TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act, enacted on November 25, 2002 (Pub. L. No. 107-296, 116 Stat. 2135, 2178 (2002)).

[25] Prior to TWIC, facilities and vessels administered their own approaches for controlling access based on the perceived risk at the facility. These approaches, among others, included requiring people seeking access to have a reason for entering, facility-specific identification, and in some cases, a background check. Some ports and port facilities still maintain their own credentials.

[26] Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295,116 Stat. 2064 (2002)). The FBI estimates that in the United States, cargo crime amounts to $12 billion annually and finds that most cargo theft occurs in or near seaports.

[27] U.S. Coast Guard Intelligence Coordination Center, *National Maritime Terrorism Threat Assessment* (Washington, D.C.: Jan. 7, 2008).

Guard assessment, al Qaeda-inspired operatives are most likely to use vehicle bombs to strike U.S. cargo vessels, tankers, and fixed coastal facilities such as ports. Studies have demonstrated that attacks on ports could have serious consequences. For example, a study by the Center for Risk and Economic Analysis of Terrorist Events on the impact of a dirty bomb attack on the Ports of Los Angeles and Long Beach estimated that the economic consequences from a shutdown of the harbors due to the contamination could result in significant losses in the tens of billions of dollars, including the decontamination costs and the indirect economic impacts due to the port shutdown.[28]

As defined by DHS, the purpose of the TWIC program is to design and field a common credential for all transportation workers across the United States who require unescorted access to secure areas at MTSA-regulated maritime facilities and vessels.[29] As such, the TWIC program, once implemented, aims to meet the following stated mission needs:

- Positively identify authorized individuals who require unescorted access to secure areas of the nation's transportation system.
- Determine the eligibility of individuals to be authorized unescorted access to secure areas of the transportation system by conducting a security threat assessment.
- Ensure that unauthorized individuals are not able to defeat or otherwise compromise the access system in order to be granted permissions that have been assigned to an authorized individual.
- Identify individuals who fail to maintain their eligibility requirements subsequent to being permitted unescorted access to secure areas of the nation's transportation system and immediately revoke the individual's permissions.

[28] H. Rosoff and D. von Winterfeldt, "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach," *Journal of Risk Analysis*, vol. 27, no. 3 (2007). This research was supported by DHS through the Center for Risk and Economic Analysis of Terrorist Events by grant funding.

[29] This is defined in the TWIC System Security Plan and the DHS Budget Justification to Congress for fiscal years 2009 and 2010.

TWIC Program Processes for Ensuring TWIC-Holder Eligibility

TSA is responsible for enrolling TWIC applicants and conducting background checks to ensure that only eligible individuals are granted TWICs.[30] In addition, pursuant to TWIC-related regulations, MTSA-regulated facility and vessel operators are responsible for reviewing each individual's TWIC as part of their decision to grant unescorted access to secure areas of their facilities. The Coast Guard is responsible for assessing and enforcing operator compliance with TWIC-related laws and regulations. Described below are key components of each process for ensuring TWIC-holder eligibility.

Enrollment: Transportation workers are enrolled by providing biographic information, such as name, date of birth, and address, and proof of identity documents, and then being photographed and fingerprinted at enrollment centers by trusted agents. A trusted agent is a member of the TWIC team who has been authorized by the federal government to enroll transportation workers in the TWIC program and issue TWIC cards.[31] Appendix I summarizes key steps in the enrollment process.

Background checking: TSA conducts background checks on each worker who applies for a TWIC to ensure that individuals who enroll do not pose a security risk to the United States. A worker's potential link to terrorism, criminal history, immigration status, and mental capacity are considered as part of the security threat assessment. Workers have the opportunity to appeal negative results of the threat assessment or request a waiver of certain specified criminal offenses, and immigration or mental capacity standards. Specifically, the TWIC background checking process includes two levels of review.

> **First-level review: Initial automated background checking.** The initial automated background checking process is conducted to determine whether any derogatory information is associated with the name and fingerprints submitted by an applicant during

[30] TWIC program threat assessment processes include conducting a background check to determine whether each TWIC 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.

[31] Trusted agents are subcontractor staff acquired by Lockheed Martin as part of its support contract with TSA for the TWIC program.

the enrollment process. This check is conducted against the FBI's criminal history records. These records contain information from federal and state and local sources in the FBI's National Crime Information Center (NCIC) database and the FBI's Integrated Automated Fingerprint Identification System (IAFIS)/Interstate Identification Index (III), which maintain criminal records and related fingerprint submissions. Rather than positively confirming each individual's identity using the submitted fingerprints, the FBI's criminal history records check is a negative identification check, whereby the fingerprints are used to confirm that the associated individual is not on the FBI criminal history list. If an individual is identified as being on the FBI's criminal history list, relevant information is to be forwarded to TSA for adjudication.[32] The check is also conducted against federal terrorism information from the Terrorist Screening Database, including the Selectee and No-Fly Lists.[33] To determine an applicant's immigration/citizenship status and eligibility, TSA also runs applicant information against the Systematic Alien Verification for Entitlements (SAVE) system. If the applicant is identified as a U.S.-born citizen with no related derogatory information, the system can approve the issuance of a TWIC with no further review of the applicant or human intervention.

Second-level review: TSA's 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

[32] Not all TWIC applicants will have readable fingerprints. As we have previously reported, it is estimated that about 2 percent to 5 percent of people cannot be easily fingerprinted because their fingerprints have become dry or worn from age, extensive manual labor, or exposure to corrosive chemicals (See GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[33] 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 terrorist screening database (the watch list) and to provide for the use of watch-list records during security-related screening processes. The Selectee List contains information on individuals who should receive enhanced screening (e.g., additional physical screening or a hand-search of carry-on baggage) before proceeding through the security checkpoint at airports. The No Fly List contains information on individuals who should be precluded from boarding flights. The No Fly and Selectee lists contain applicable records from the FBI Terrorist Screening Center's consolidated database of known or appropriately suspected terrorists.

information. As such, not all TWIC applicants will be subjected to a second-level review. The second-level review consists of staff at TSA's adjudication center reviewing the applicant's enrollment file.[34]

Card use and compliance: Once a TWIC has been activated and issued, the worker may present his or her TWIC to security officials when he or she seeks unescorted access to a secure area. Currently, visual inspections of TWICs are required for controlling access to secure areas of MTSA-regulated facilities and vessels.[35] Approaches for inspecting TWICs using biometric readers at individual facilities and vessels across the nation are being considered as part of a pilot but are not yet required. Pursuant to Coast Guard policy,[36] Coast Guard inspectors are required to verify TWIC cards during annual compliance exams, security spot checks, and in the course of other Coast Guard duties as determined by the Captain of the Port[37] based on risk and resource availability. The Coast Guard's primary means of verification is shifting toward the use of biometric handheld readers with the continued deployment of readers to each of its Sectors

[34] If an applicant has asserted him/herself to be a non-U.S. citizen or non-U.S.-born citizen, TSA staff at the adjudication center are to positively identify the individual by confirming aspects of the individual's biographic information, inclusive of their alien registration number and other physical descriptors, against available databases. For those individuals, TSA requires that at least one of the documents provided as proof of identity demonstrates immigration status or United States citizenship. According to TWIC officials, the program is able to validate immigration status and citizenship-related documents required of noncitizens and non-U.S.-born citizens—such as certificates of naturalization—with the originating source. For individuals with derogatory information, staff at the adjudication center reviews each applicant's file to determine if the derogatory information accurately applies to the individual or includes disqualifying information.

[35] Coast Guard regulations require that such an inspection include (1) a match of the photo on the TWIC to the individual presenting the TWIC, (2) verification that the TWIC has not expired, and (3) a visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

[36] See United States Coast Guard, Commandant Instruction Manual 16601.1: *Coast Guard Transportation Worker Identification Credential (TWIC) Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

[37] The Captain of the Port is the Coast Guard officer designated by the Commandant to enforce within his or her respective areas port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

and Marine Safety Units.[38] As of December 21, 2010, the Coast Guard reports to have deployed biometric handheld readers to all of its 35 Sectors and 16 Marine Safety Units.

TWIC Regulations and Cost

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.[39]

To inform the rulemaking process, TSA initiated a pilot in August 2008, known as the TWIC reader pilot, to test TWIC-related access control technologies.[40] This pilot is intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. As such, the pilot is expected to test the feasibility and functionality of using TWICs with biometric card readers within the maritime environment. After the pilot has concluded, a report on the findings of the pilot is expected to inform the development of the card reader rule. DHS currently estimates that a notice of proposed rulemaking will be issued late in calendar year 2011 and that the final rule will be promulgated no earlier than the end of calendar year 2012.

[38] Coast Guard Sectors run all Coast Guard missions at the local and port levels, such as search and rescue, port security, environmental protection, and law enforcement in ports and surrounding waters, and oversee a number of smaller Coast Guard units, including small cutters and small-boat stations.

[39] 74 Fed. Reg. 13360 (2009). An advanced notice of proposed rulemaking is published in the *Federal Register* and contains notices to the public of the proposed issuance of rules and regulations. The purpose of this advanced notice of proposed rulemaking was to encourage the discussion of potential TWIC reader requirements prior to the rulemaking process.

[40] The pilot initiation date is based on the first date of testing identified in the TWIC pilot schedule. This date is not inclusive of time taken for planning the pilot prior to the first test. The SAFE Port Act required the pilot to commence no later than 180 days after the date of enactment (Oct. 13, 2006) of the SAFE Port Act. See GAO-06-982.

According to agency officials, from fiscal years 2002 through 2010, the TWIC program had funding authority totaling $420 million. In issuing the credential rule, DHS estimated that implementing the TWIC program could cost the federal government and the private sector a combined total of between $694.3 million and $3.2 billion over a 10-year period. However, these figures did not include costs associated with implementing and operating readers.[41] Appendix II contains additional program funding details.

Standards for Internal Control

Standards for Internal Control in the Federal Government underscores the need for developing effective controls for meeting program objectives and complying with applicable regulations.[42] Effective internal controls provide for an assessment of the risks the agency faces from both internal and external sources. Once risks have been identified, they should be analyzed for their possible effect. Management then has to decide upon the internal control activities required to mitigate those risks and achieve the objectives of efficient and effective operations. As part of this effort, management should design and implement internal controls based on the related cost and benefits.

In addition, internal control standards highlight the need for the following:

- capturing information needed to meet program objectives;
- designing controls to assure that ongoing monitoring occurs in the course of normal operations;
- determining that relevant, reliable, and timely information is available for management decision-making purposes;
- conducting reviews and testing of development and modification activities before placing systems into operation;
- recording and communicating information to management and others within the entity who need it and in a form and within a time frame that enables them to carry out their internal control and other responsibilities; and
- designing internal controls to provide reasonable assurance that compliance with applicable laws and regulations is being achieved, and provide appropriate supervisory review of activities to help provide

[41] See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule, 72 Fed. Reg. 3492, 3571 (2007).

[42] GAO/AIMD-00-21.3.1.

oversight of operations. This includes designing and implementing appropriate supervisory review activities to help provide oversight and analyzing data to compare trends in actual performance to expected results to identify any areas that may require further inquiries or corrective action.

Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. An internal control weakness is a condition within an internal control system worthy of attention. A weakness, therefore, may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen internal controls to provide a greater likelihood that the entity's objectives will be achieved.

Internal Control Weaknesses in DHS's Biometric Transportation ID Program Hinder Efforts to Ensure Security Objectives Are Fully Achieved

DHS has established a system of TWIC-related processes and controls. However, internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals. Specifically, internal controls[43] in the enrollment and background checking processes are not designed to provide reasonable assurance that (1) only qualified individuals can acquire TWICs; (2) adjudicators follow a process with clear criteria for applying discretionary authority when applicants are found to have extensive criminal convictions; or (3) once issued a TWIC, TWIC holders have maintained their eligibility. To meet the stated program mission needs, TSA designed TWIC program processes to facilitate the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls designed and in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. Further, internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of selected MTSA-regulated facilities during covert tests conducted by our investigators.

[43] In accordance with *Standards for Internal Control in the Federal Government*, the design of the internal controls is to be informed by identified risks the program faces from both internal and external sources; the possible effect of those risks; control activities required to mitigate those risks; and the cost and benefits of mitigating those risks.

TWIC Program Controls Are Not Designed to Provide Reasonable Assurance That Only Qualified Applicants Can Acquire TWICs

DHS has established a system of TWIC-related processes and controls that as of April 2011 has resulted in TWICs being denied to 1,158 applicants based on a criminal offense, criminal immigration offense, or invalid immigration status.[44] However, the TWIC program's internal controls for positively identifying an applicant, arriving at a security threat determination for that individual, and approving the issuance of a TWIC, are not designed to provide reasonable assurance that only qualified applicants can acquire TWICs.[45] Assuring the identity and qualifications of TWIC-holders are two of the primary benefits that the TWIC program is to provide MTSA-regulated facility and vessel operators making access control decisions. If an individual presents an authentic TWIC acquired through fraudulent means when requesting access to the secure areas of a MTSA-regulated facility or vessel, the cardholder is deemed not to be a security threat to the maritime environment because the cardholder is presumed to have met TWIC-related qualifications during a background check. In such cases, these individuals could better position themselves to inappropriately gain unescorted access to secure areas of a MTSA-regulated facility or vessel.[46]

As confirmed by TWIC program officials, there are ways for an unqualified individual to acquire an authentic TWIC. According to TWIC program officials, to meet the stated program purpose, TSA's focus in designing the TWIC program was on facilitating the issuance of TWICs to maritime workers. However, TSA did not assess internal controls prior to implementing the program. Further, prior to fielding the program, TSA did not conduct a risk assessment of the TWIC program to identify program risks and the need for controls to mitigate existing risks and weaknesses, as called for by internal control standards. Such an assessment could help

[44] TSA further reports that as of April 2011 there have been 34,503 cases out of 1,841,122 enrollments, or 1.9 percent of TWIC enrollments, where enrollees have not been approved for a TWIC because TSA has identified that the enrollees have at least one potentially disqualifying criminal offense, criminal immigration offense, or invalid immigration status, and the enrollee did not respond to an initial determination of threat assessment. Under the TWIC vetting process, an applicant that receives an initial determination of threat assessment is permitted to provide additional information to respond to or challenge the determination, or to request a waiver for the disqualifying condition, and subsequently be granted a TWIC.

[45] For the purposes of this report, routinely is defined as a process being consistently applied in accordance with established procedure so as to render consistent results.

[46] The TWIC program requires individuals to both hold a TWIC and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and vessels.

provide reasonable assurance that control weaknesses in one area of the program do not undermine the reliability of other program areas or impede the program from meeting mission needs. TWIC program officials told us that control weaknesses were not addressed prior to initiating the TWIC program because they had not previously identified them, or because they would be too costly to address. However, officials did not provide documentation to support their cost concerns and told us that they did not complete an assessment that accounted for whether the program could achieve defined mission needs without implementing additional or compensating controls to mitigate existing risks, or the risks associated with not correcting for existing internal control weaknesses.

Our investigators conducted covert tests at enrollment center(s) to help test the rigor of the TWIC enrollment and background checking processes. The investigators fully complied with the enrollment application process. They were photographed and fingerprinted, and asserted themselves to be U.S.-born citizens.[47] The investigators were successful in obtaining authentic TWIC cards despite going through the background-checking process. Not having internal controls designed to provide reasonable assurance that the applicant has (1) been positively identified, and (2) met all TWIC eligibility requirements, including not posing a security threat to MTSA-regulated facilities and vessels, could have contributed to the investigators' successes. Specifically, we identified internal control weaknesses in the following three areas related to ensuring that only qualified applicants are able to obtain a TWIC.

Controls to identify the use of potentially counterfeit identity documents are not used to inform background checking processes. As part of TWIC program enrollment, a trusted agent is to review identity documents for authenticity and use an electronic authentication device to assess the likelihood of the document being counterfeit.[48] According to TWIC program officials, the trusted agent's review of TWIC applicant identity documents and the assessment provided by the electronic authentication device are the two steps intended to serve as the primary

[47] The details related to the means used by the investors in the tests could not be detailed here because they were deemed sensitive security information by TSA.

[48] As designed, the TWIC program's enrollment process relies on a trusted agent—a contract employee—to collect an applicant's identification information. The trusted agent is provided basic training on how to detect a fraudulent document. The training, for example, consists of checking documents for the presence of a laminate that is not peeling, typeset that looks legitimate, and seals on certain types of documents.

controls for detecting whether an applicant is presenting counterfeit identity documents. Additionally, the electronic device used to assess the authenticity of identification credentials renders a score on the likelihood of the document being authentic and produces an assessment report in support of the score. Assessing whether the applicant's credential is authentic is one source of information for positively identifying an applicant. Our investigators provided counterfeit or fraudulently acquired documents, but they were not detected.

However, the TWIC program's background checking processes are not designed to routinely consider the results of controls in place for assessing whether an applicant's identity documents are authentic. For example, assessments of document authenticity made by a trusted agent or the electronic document authentication device as part of the enrollment process are not considered as part of the first-level background check. Moreover, TWIC program officials agree that this is a program weakness. As of December 1, 2010, approximately 50 percent of TWICs were approved after the first-level background check without undergoing further review.[49] As an initial step towards addressing this weakness, and in response to our review, TWIC program officials told us that since April 17, 2010, the comments provided at enrollment by trusted agents have been sent to the Screening Gateway—a TSA system for aggregating threat assessment data. However, this change in procedure does not correct the internal control weaknesses we identified.[50] Attempts to authenticate copies of documents are limited because it is not possible to capture all of the security features when copies of the identity documents are recorded, such as holograms or color-shifting ink. Using information on the authenticity of identity documents captured during enrollment to inform the background check could help TSA better assess the reliability and authenticity of such documents provided at enrollment.

[49] Of the 1,697,160 enrollments approved for a TWIC, 852,540 were approved using TSA's automated process as part of the first-level background check without undergoing further review.

[50] Details from this section were removed because the agency deemed them sensitive security information.

Controls related to the legal status of self-reported U.S.-born citizens or nationals.[51] The TWIC program does not require that applicants claiming to be U.S.-born citizens or nationals provide identity documents that demonstrate proof of citizenship, or lawful status in the United States. See appendix III for the list of documents U.S.-born citizens or nationals must select from and present when applying for a TWIC.[52] For example, an applicant could elect to provide one document, such a U.S. passport, which, according to TSA officials, serves as proof of U.S. citizenship or proof of nationality. However, an applicant could elect to submit documents that do not provide proof of citizenship. As of December 1, 2010, nearly 86 percent of approved TWIC enrollments were by self-identified United States citizens or nationals asserting that they were born in the United States or a United States territory.[53]

Verifying a U.S.-born citizen's identity and related lawful status can be costly and is a challenge faced by U.S. government programs such as passports.[54] However, reaching an accurate determination of a TWIC applicant's potential security threat in meeting TWIC mission needs is dependant on positively identifying the applicant. Given such potential cost constraints, consistent with internal control standards, identifying alternative mechanisms to positively identify individuals to the extent that the benefits exceed the costs and TWIC program mission needs are met could enhance TSA's ability to positively identify individuals and reduce the likelihood that criminals or terrorists could acquire a TWIC fraudulently.

[51] National means a citizen of the United States or a noncitizen owing permanent allegiance to the United States. In general, U.S.-born nationals who are not U.S. citizens at birth are individuals born in an outlying possession of the United States. Details from this section were removed because the agency deemed them sensitive security information.

[52] Various identity documents can be provided by U.S.-born citizens or nationals when applying for a TWIC. For certain documents, such as an unexpired U.S. passport, TSA requires one document as a proof of identity. For other documents, such as a Department of Transportation Medical Card or United States Military Dependents Identification Card, TSA requires that TWIC applicants provide two identity documents from a designated list, with one being a government-issued photo identification.

[53] As of December 1, 2010, TSA reported that 1,697,160 TWIC enrollments have been approved, of which 1,457,337 were self-identified United States citizens or nationals asserting that they were born in the United States or in a United States territory.

[54] See GAO, *State Department: Significant Vulnerabilities in the Passport Issuance Process*, GAO-09-681T (Washington, D.C.: May 5, 2009) and *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, GAO-05-477 (Washington, D.C.: May 20, 2005).

Controls are not in place to determine whether an applicant has a need for a TWIC.[55] Regulations governing the TWIC program security threat assessments require applicants to disclose their job description and location(s) where they will most likely require unescorted access, if known, and the name, telephone number, and address of the applicant's current employer(s) if the applicant works for an employer that requires a TWIC.[56] However, TSA enrollment processes do not require that this information be provided by applicants. For example, when applying for a TWIC, applicants are to certify that they may need a TWIC as part of their employment duties. However, the enrollment process does not request information on the location where the applicant will most likely require unescorted access, and enrollment processes include asking the applicant if they would like to provide employment information, but informing the applicant that employer information is not required.

While not a problem prior to implementing the TWIC program, according to TSA officials, a primary reason for not requiring employer information be captured by applicant processes is that many applicants do not have employers, and that many employers will not accept employment applications from workers who do not already have a TWIC. However, TSA could not provide statistics on (1) how many individuals applying for TWICs were unemployed at the time of their application; or (2) a reason why the TWIC-related regulation does not prohibit employers from denying employment to non-TWIC holders who did not previously have a

[55] TWIC is unlike other federally-sponsored access control credentials, such as the Department of Defense's Common Access Card—the agencywide standard identification card—for which sponsorship by an employer is required. For these federal credentialing programs, employer sponsorship begins with the premise that an individual is known to need certain access as part of their employment. Further, the employing agency is to conduct a background investigation on the individual and has access to other personal information, such as prior employers, places of residency, and education, which they may confirm as part of the employment process and use to establish the individual's identity.

[56] Implementing regulations at 49 C.F.R. § 1572.17 require that when applying for or renewing a TWIC, the applicant provide, among other information: (1) the reason that the applicant requires a TWIC, including, as applicable, the applicant's job description and the primary facility, vessel, or maritime port location(s) where the applicant will most likely require unescorted access, if known; (2) the name, telephone number, and address of the applicant's current employer(s) if the applicant works for an employer that requires a TWIC; and (3) if the applicant works for an employer that does not require possession of a TWIC, does not have a single employer, or is self-employed, the primary vessel or port location(s) where the applicant requires unescorted access, if known. The regulation states that this information is required to establish eligibility for a TWIC and that TSA is to review the applicant information as part of the intelligence-related check.

need for a TWIC. Further, according to TSA and Coast Guard officials, industry was opposed to having employment information verified as part of the application process, as industry representatives believed such checks would be too invasive and time-consuming. TSA officials further told us that confirming this information would be too costly.

We recognize that implementing mechanisms to capture this information could be time-consuming and involve additional costs. However, collecting information on present employers or operators of MTSA-regulated facilities and vessels to be accessed by the applicant, to the extent that the benefits exceed the costs and TWIC program mission needs are met, could help ensure TWIC program mission needs are being met, and serve as a barrier to individuals attempting to acquire an authentic TWIC through fraudulent means. Therefore, if TSA determines that implementing such mechanisms are, in fact, cost prohibitive, identifying and implementing appropriate compensating controls could better position TSA to positively identify the TWIC applicant. Not taking any action increases the risk that individuals could gain unescorted access to secure areas of MTSA-regulated facilities and vessels.

As of September 2010, TSA's background checking process had identified no instances of nonimmigration-related document or identity fraud. This is in part because of previously discussed weaknesses in TWIC program controls for positively identifying applicants, and the systems and procedures the TWIC program relies on not being designed to effectively monitor for such occurrences, in accordance with internal control standards. Though not an exhaustive list, through a review of Coast Guard reports and publicly available court records, we identified five court cases where the court documents indicate that illegal immigrants acquired, or in one of the cases sought to acquire, an authentic TWIC through fraudulent activity such as providing fraudulent identity information and, in at least one of the cases and potentially up to four, used the TWIC to access secure areas of MTSA-regulated facilities. Four of these cases were a result of, or involved, United States Immigration and Customs Enforcement efforts after individuals had acquired, or sought to acquire, a TWIC. As of September 2010, the program's background checking process identified 18 instances of potential fraud out of the approximately 1,676,000 TWIC enrollments. These instances all involved some type of

fraud related to immigration.[57] The 18 instances of potential fraud were identified because the 18 individuals asserted themselves to be non-U.S.-born applicants and, unlike processes in place for individuals asserting to be U.S.-born citizens, TSA's background checking process includes additional controls to validate such individuals' identities. For example, TSA requires that at least one of the documents provided by such individuals at enrollment show proof of their legal status and seeks to validate each non-U.S.-born applicant's identity with the U.S. Citizenship and Immigration Services.

Internal control standards highlight the need for capturing information needed to meet program objectives; ensuring that relevant, reliable, and timely information is available for management decision-making purposes; and providing reasonable assurance that compliance with applicable laws and regulations is being achieved.[58] Conducting a control assessment of the TWIC program's processes to address existing weaknesses could enhance the TWIC program's ability to prevent and detect fraud and positively identify TWIC applicants. Such an assessment could better position DHS in strengthening the program to ensure it achieves its objectives in controlling access to MTSA-regulated facilities and vessels.

[57] According to TSA, as of September 8, 2010, a total of 18 TWIC applicants were issued an Initial Determination of Threat Assessment for invalid immigration documents. Upon submission to the U.S. Citizenship and Immigration Services, the documentation was reported to be altered or counterfeit. Of these 18 instances, only 1 applicant submitted additional documentation following an Initial Determination of Threat Assessment to challenge TSA's determination. The single applicant was subsequently awarded a TWIC.

[58] GAO/AIMD-00-21.3.1.

TWIC Program Controls Are Not Designed to Require Adjudicators to Follow a Process with Clear Criteria for Applying Discretionary Authority When Applicants Are Found to Have Extensive Criminal Convictions

Being convicted of a felony does not automatically disqualify a person from being eligible to receive a TWIC; however, prior convictions for certain crimes are automatically disqualifying. Threat assessment processes for the TWIC program include conducting background checks to determine whether each TWIC applicant poses a security threat.[59] Some of these offenses, such as espionage or treason, would permanently disqualify an individual from obtaining a TWIC. Other offenses, such as murder or the unlawful possession of an explosive device, while categorized as permanent disqualifiers, are also eligible for a waiver under TSA regulations and might not permanently disqualify an individual from obtaining a TWIC if TSA determines upon subsequent review that an applicant does not represent a security threat.[60] Table 1 presents examples of disqualifying criminal offenses set out in statute and implementing regulations for consideration as part of the adjudication process.

[59] These checks, in general, can include checks for criminal history records, immigration status, terrorism databases and watchlists, and records indicating an adjudication of a lack of mental capacity, among other things. As defined in TSA implementing regulations, the term security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism. 49 C.F.R. § 1570.3.

[60] These permanent disqualifying offenses for which no waiver can be issued include espionage, sedition, treason, a federal crime of terrorism, or conspiracy to commit any of these offenses.

Table 1: Examples of Disqualifying Offenses for TWIC Eligibility

Permanent disqualifying offenses[a]	Permanent disqualifying offenses that can be waived[b]	Interim disqualifying offenses[c]
Espionage	Murder	Bribery
Sedition	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device	Smuggling
Treason		Arson
A federal crime of terrorism		Extortion
		Robbery
	A crime involving a transportation security incident	
	Making any threat 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	

Source: GAO analysis of regulations and TSA.

Notes: See appendix IV for a list of all disqualifying offenses.

[a]Permanent disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(a) for which no waiver can be granted under 49 C.F.R. 1515.7(a)(i).

[b]Permanent disqualifying offenses that can be waived are offenses defined in 49 C.F.R. 1572.103(a) for which a waiver can be granted in accordance with 49 C.F.R. 1515.7(a)(i). Applicants with certain permanent criminal offenses and all interim disqualifying criminal offenses may request a waiver of their disqualification. TSA regulations provide that in determining whether to grant a waiver, TSA will consider (1) the circumstances of the disqualifying act or offense; (2) restitution made by the applicant; (3) any federal or state mitigation remedies; (4) court records or official medical release documents indicating that the applicant no longer lacks mental capacity; and (5) other factors that indicate the applicant does not pose a security threat warranting denial of a hazardous materials endorsement or TWIC.

[c]Interim disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(b) for which the applicant has either been (1) convicted, or found not guilty by reason of insanity, within a 7-year period preceding the TWIC application, or (2) incarcerated for within a 5-year period preceding the TWIC application.

TSA also has the authority to add to or modify the list of interim disqualifying crimes. Further, in determining whether an applicant poses a security threat, TSA officials stated that adjudicators have the discretion to consider the totality of an individual's criminal record, including criminal offenses not defined as a permanent or interim disqualifying criminal offenses, such as theft or larceny.[61] More specifically, TSA's

[61] The U.S. government's Adjudicative Desk Reference, used in adjudicating security clearances, states that multiple criminal offenses indicate intentional continuing behavior that raises serious questions about a person's trustworthiness and judgment.

implementing regulations provide, in part, that with respect to threat assessments, TSA may determine that an applicant poses a security threat if the search conducted reveals extensive foreign or domestic criminal convictions, a conviction for a serious crime not listed as a permanent or interim disqualifying offense, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days. Thus, if a person was convicted of multiple crimes, even if each of the crimes were not in and of themselves disqualifying, the number and type of convictions could be disqualifying.

Although TSA has the discretion and authority to consider criminal offenses not defined as a disqualifying offense, such as larceny and theft, and periods of imprisonment, TSA has not developed a definition for what extensive foreign or domestic criminal convictions means, or developed guidance to ensure that adjudicators apply this authority consistently in assessing the totality of an individual's criminal record. For example, TSA has not developed guidance or benchmarks for adjudicators to consistently apply when reviewing TWIC applicants with extensive criminal convictions but no disqualifying offense. This is particularly important given TSA's reasoning for including this authority in TWIC-related regulation. Specifically, TSA noted that it understands that the flexibility this language provides must be used cautiously and on the basis of compelling information that can withstand judicial review. They further noted that the decision to determine whether an applicant poses a threat under this authority is largely a subjective judgment based on many facts and circumstances.

While TSA does not track metrics on the number of TWICs provided to applicants with specific criminal offenses not defined as disqualifying offenses, as of September 8, 2010, the agency reported 460,786 cases where the applicant was approved, but had a criminal record based on the results from the FBI. This represents approximately 27 percent of individuals approved for a TWIC at the time. In each of these cases, the applicant had either a criminal offense not defined as a disqualifying offense or an interim disqualifying offense that was no longer a disqualification based on conviction date or the applicant's release date from incarceration. Consequently, based on TSA's background checking procedures, all of these cases would have been reviewed by an adjudicator for consideration as part of the second-level background check because derogatory information had been identified. As such, each of these cases had to be examined and a judgment had to be made as to whether to deny an applicant a TWIC based on the totality of the offenses contained in each applicant's criminal report.

While there were 460,786 cases where the applicant was approved, but had a criminal record, TSA reports to have taken steps to deny 1 TWIC applicant under this authority. However, in the absence of guidance for the application of this authority, it is not clear how TSA applied this authority in approving the 460,786 applications and denying the 1. Internal control standards call for controls and other significant events to be clearly documented in directives, policies, or manuals to help ensure operations are carried out as intended.

According to TSA officials, the agency has not implemented guidance for adjudicators to follow on how to apply this discretion in a consistent manner because they are confident that the adjudicators would, based on their own judgment, identify all applicants where the authority to deny a TWIC based on the totality of all offenses should be applied. However, in the absence of criteria, we were unable to analyze or compare how the approximately 30 adjudicators who are assigned to the TWIC program at any given time made determinations about TWIC applicants with extensive criminal histories. Given that 27 percent of TWIC holders have been convicted of at least one nondisqualifying offense, defining what extensive criminal convictions means and developing guidance or criteria for how adjudicators should apply this discretionary authority could help provide TSA with reasonable assurance that applications are consistently adjudicated. Defining terms and developing guidance is consistent with internal control standards.

TWIC Program Controls Are Not Designed to Provide Reasonable Assurance That TWIC Holders Have Maintained Their Eligibility Once Issued TWICs

DHS's defined mission needs for TWIC include identifying individuals who fail to maintain their eligibility requirements once issued a TWIC, and immediately revoking the individual's card privileges. Pursuant to TWIC-related regulations, an individual may be disqualified from holding a TWIC and be required to surrender the TWIC to TSA for failing to meet certain eligibility criteria related to, for example, terrorism, crime, and immigration status. However, weaknesses exist in the design of the TWIC program's internal controls for identifying individuals who fail to maintain their eligibility that make it difficult for TSA to provide reasonable assurance that TWIC holders continue to meet all eligibility requirements.

Controls are not designed to determine whether TWIC holders have committed disqualifying crimes at the federal or state level after being granted a TWIC. TSA conducts a name-based check of TWIC holders against federal wants[62] and warrants on an ongoing basis. According to FBI and TSA officials, policy and statutory provisions hamper the program from running the broader FBI fingerprint-based check using the fingerprints collected at enrollment on an ongoing basis. More specifically, because the TWIC background check is considered to be for a noncriminal justice purpose,[63] to conduct an additional fingerprint-based check as part of an ongoing TWIC background check, TSA would have to collect a new set of fingerprints from the TWIC-holder,[64] if the prints are more than 1 year old, and submit those prints to the FBI each time they want to assess the TWIC-holder's criminal history. According to TSA officials, it would be cost prohibitive to run the fingerprint-based check on an ongoing basis, as TSA would have to pay the FBI $17.25 per check.

Although existing policies may hamper TSA's ability to check FBI-held fingerprint-based criminal history records for the TWIC program, TSA has not explored alternatives for addressing this weakness, such as informing facility and port operators of this weakness and identifying solutions for leveraging existing state criminal history information, where available. For instance, state maritime organizations may have other mechanisms at their disposal for helping to identify TWIC-holders who may no longer meet TWIC qualification requirements. Specifically, laws governing the maritime environment in New York and New Jersey provide for credentialing authorities being notified if licensed or registered longshoremen have been arrested. Further, other governing entities, such as the State of Florida and

[62] Federal wants generally consist of information on wanted persons, or individuals, for whom federal warrants are outstanding.

[63] Under the National Crime Prevention and Privacy Compact Act of 1998 (Pub. L. No. 105-251, 112 Stat. 1870, 1874 (1998) (codified as amended at 42 U.S.C. §§ 14601-14616)), which established an infrastructure by which states and other specified parties can exchange criminal records for noncriminal justice purposes authorized under federal or state law, 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, licensing determinations, immigration and naturalization matters, and national security clearances.

[64] Under the 1998 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.

the Alabama State Port Authority, have access to state-based criminal records checks. While TSA may not have direct access to criminal history records, TSA could compensate for this control weakness, for example, by leveraging existing mechanisms available to maritime stakeholders across the country to better ensure that only qualified individuals retain TWICs.

Controls are not designed to provide reasonable assurance that TWIC holders continue to meet immigration status eligibility requirements. If a TWIC holder's stated period of legal presence in the United States is about to expire or has expired, the TWIC program does not request or require proof from TWIC holders to show that they continue to maintain legal presence in the United States. Additionally, although they have the regulatory authority to do so, the program does not issue TWICs for a term less than 5 years to match the expiration of a visa. Instead, TSA relies on (1) TWIC holders to self-report if they no longer have legal presence in the country, and (2) employers to report if a worker is no longer legally present in the country.[65] As we have previously reported, government programs for granting benefits to individuals face challenges in confirming an individual's immigration status.[66] TWIC program officials stated that the program uses a United States Citizenship and Immigration Services system during the background checking process prior to issuing a TWIC as a method for confirming the legal status of non-U.S. citizens.[67] TSA has not, however, consistent with internal control standards,

[65] TWIC-related regulations provide, for example, that individuals disqualified from holding a TWIC for immigration status reasons must surrender the TWIC to TSA. In addition, the regulations provide that TWICs are deemed to have expired when the status of certain lawful nonimmigrants with a restricted authorization to work in the United States (e.g., H-1B1 Free Trade Agreement) expires, the employer terminates the employment relationship with such an applicant, or such applicant otherwise ceases working for the employer, regardless of the date on the face of the TWIC. Upon the expiration of such nonimmigrant status for an individual who has a restricted authorization to work in the United States, the employer and employee both have related responsibilities—the employee is required to surrender the TWIC to the employer, and the employer is required to retrieve the TWIC and provide it to TSA. According to TSA officials, the TWIC program could not provide a count of the total number of TWIC holders whose employers reported that the TWIC holders no longer have legal status, as they do not track this information.

[66] See, for example, GAO, *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Washington, D.C.: Dec. 17, 2010), and *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO-05-813 (Washington, D.C.: Aug. 31, 2005).

[67] Details from this section were removed because the agency deemed them sensitive security information.

implemented alternative controls to compensate for this limitation and provide reasonable assurance that TWIC holders remain eligible. For instance, the TWIC program has not compensated for this limitation by (1) using its authority to issue TWICs with shorter expiration dates to correspond with each individual's legal presence, or (2) updating the TWIC system to systematically suspend TWIC privileges for individuals who no longer meet immigration eligibility requirements until they can provide evidence of continued legal presence.[68]

TWIC program officials stated that implementing these compensating measures would be too costly, but they have not conducted an assessment to identify the costs of implementing these controls, or determined if the benefits of mitigating related security risks would outweigh those costs, consistent with internal control standards. Not implementing such measures could result in a continued risk of individuals no longer meeting TWIC legal presence requirements continuing to hold a federally issued identity document and gaining unescorted access to secure areas of MTSA-regulated facilities and vessels.[69] Thus, implementing compensating measures, to the extent that the benefits outweigh the costs and meet the program's defined mission needs, could provide TSA, the Coast Guard, and MTSA-regulated stakeholders with reasonable assurance that each TWIC holder continues to meet TWIC-related eligibility requirements.

Internal Control Weaknesses in TWIC Enrollment, Background Checking, and Use Could Have Contributed to Breach of MTSA-Regulated Ports

As of January 7, 2011, the Coast Guard reports that it has identified 11 known attempts to circumvent TWIC requirements for gaining unescorted access to MTSA-regulated areas by presenting counterfeit TWICs. The Coast Guard further reports to have identified 4 instances of individuals presenting another person's TWIC as their own in attempts to gain access. Further, our investigators conducted covert tests to assess the use of TWIC as a means for controlling access to secure areas of MTSA-regulated facilities. During covert tests of TWIC at several selected ports, our investigators were successful in accessing ports using counterfeit TWICs,

[68] The TWIC program accepts various documents, such as visas, Interim Employment Authorizations, and form I-94 Arrival and Departure Records, as evidence of legal presence in the United States.

[69] TWIC is a federally issued identity document that can be used as proof of identity for nonmaritime activities, such as boarding airplanes at United States airports and certain Department of Defense facilities in accordance with Department of Defense policy, Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DOD Physical Access Control," dated December 8, 2009.

authentic TWICs acquired through fraudulent means, and false business cases (i.e., reasons for requesting access).[70] Our investigators did not gain unescorted access to a port where a secondary port specific identification was required in addition to the TWIC.

In response to our covert tests, TSA and Coast Guard officials stated that, while a TWIC card is required for gaining unescorted access to secure areas of a MTSA-regulated facility, the card alone is not sufficient. These officials stated that the cardholder is also required to present a business case, which security officials at facilities must consider as part of granting the individual access. In addition, according to DHS's Screening Coordination Office, a credential is only one layer of a multilayer process to increase security. Other layers of security might include onsite law enforcement, security personnel, cameras, locked doors and windows, alarm systems, gates, and turnstiles. Thus, a weakness in the implementation of TWIC will not guarantee access to the secure areas of a MTSA-regulated port or facility.

However, as our covert tests demonstrated, having an authentic TWIC and a legitimate business case were not always required in practice. The investigators' possession of TWIC cards provided them with the appearance of legitimacy and facilitated their unescorted entry into secure areas of MTSA-regulated facilities and ports at multiple locations across the country. If individuals are able to acquire authentic TWICs fraudulently, verifying the authenticity of these cards with a biometric reader will not reduce the risk of undesired individuals gaining unescorted access to the secure areas of MTSA-regulated facilities and vessels.

Given existing internal control weaknesses, conducting a control assessment of the TWIC program's processes to address existing weaknesses could enhance the TWIC program's ability to prevent and detect fraud and positively identify TWIC applicants. Such an assessment could better position DHS in strengthening the program to ensure it

[70] Existing vulnerabilities with TWIC to date have included, for example, problems with deteriorating TWIC card security features. Cards fading and delaminating have been reported by stakeholders across the country from places such as New York, Virginia, Texas, and California, with a range of climate conditions. According to stakeholders, these problems make it difficult for security guards to distinguish an authentic TWIC that is faded from a fraudulent TWIC. TSA and the Coast Guard have also received reports of problems with the card's chip or antenna connection not working from locations where TWICs are being used with readers. The total number of damaged TWICs with a damaged chip or antenna is unknown because TWICs are not required to be used with readers.

achieves its objectives in controlling unescorted access to MTSA-regulated facilities and vessels. It could also help DHS identify and implement the minimum controls needed to (1) positively identify individuals, (2) provide reasonable assurance that control weaknesses in one area of the program would not undermine the reliability of other program areas or impede the program from meeting mission needs, and (3) provide reasonable assurance that the threat assessments are based on complete and accurate information. Such actions would be consistent with internal control standards, which highlight the need for capturing information needed to meet program objectives; determining that relevant, reliable, and timely information is available for management decision-making purposes; and designing internal controls to provide reasonable assurance that compliance with applicable laws and regulations is being achieved, as part of implementing effective controls. Moreover, our prior work on internal controls has shown that management should design and implement internal controls based on the related costs and benefits and continually assess and evaluate its internal controls to assure that the controls being used are effective and updated when necessary.[71]

TWIC's Effectiveness at Enhancing Security Has Not Been Assessed, and the Coast Guard Lacks the Ability to Assess Trends in TWIC Compliance

The TWIC program is intended to improve maritime security by using a federally sponsored credential to enhance access controls to secure areas at MTSA-regulated facilities and vessels, but DHS has not assessed the program's effectiveness at enhancing security. In addition, Coast Guard's approach for monitoring and enforcing TWIC compliance nationwide could be improved by enhancing its collection and assessment of related maritime security information. For example, the Coast Guard tracks TWIC program compliance, but the processes involved in the collection, cataloguing, and querying of information cannot be relied on to produce the management information needed to assess trends in compliance with the TWIC program or associated vulnerabilities.

[71] GAO/AIMD-00-21.3.1.

TWIC Has Not Been Assessed to Measure Effectiveness at Enhancing Security

DHS asserted in its 2009 and 2010 budget submissions that the absence of the TWIC program would leave America's critical maritime port facilities vulnerable to terrorist activities.[72] However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Such assessments are consistent with DHS's National Infrastructure Protection Plan, which recognizes that metrics and other evaluation procedures should be used to measure progress and assess the effectiveness of programs designed to protect key assets.[73] Further, DHS has not demonstrated that TWIC, as currently implemented and planned with readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility specific identity credentials with business cases. According to TSA and Coast Guard officials, because the program was mandated by Congress as part of MTSA, DHS did not conduct a risk assessment to identify and mitigate program risks prior to implementation. Further, according to these officials, neither the Coast Guard nor TSA analyzed the potential effectiveness of TWIC in reducing or mitigating security risk—either before or after implementation—because they were not required to do so by Congress. Rather, DHS assumed that the TWIC program's enrollment and background checking procedures were effective and would not allow unqualified individuals to acquire and retain authentic TWICs.

The internal control weaknesses that we discuss earlier in the report, as well as the results of our covert tests of TWIC use, raise questions about the effectiveness of the TWIC program. According to the Coast Guard official responsible for conducting assessments of maritime risk, it may now be possible to assess TWIC effectiveness and the extent to which, or if, TWIC use could enhance security using current Maritime Security Risk

[72] See DHS, DHS Exhibit 300 Public Release BY10/TSA - Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: Apr. 17, 2009) and DHS Exhibit 300 Public Release BY09/TSA - Transportation Worker Identification Credentialing (TWIC) (Washington, D.C.: July 27, 2007).

[73] DHS, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency* (Washington, D.C.: 2009). The NIPP, first issued in June 2006 by DHS, established a six-step risk management framework to establish national priorities, goals, and requirements for Critical Infrastructure and Key Resources (CIKR) protection so that federal funding and resources are applied in the most effective manner to deter threats, reduce vulnerabilities, and minimize the consequences of attacks and other incidents. The NIPP states that comprehensive risk assessments are necessary for determining which assets or systems face the highest risk, for prioritizing risk mitigation efforts and the allocation of resources, and for effectively measuring how security programs reduce risks.

Analysis Model (MSRAM) data. Since MSRAM's deployment in 2005, the Coast Guard has used its MSRAM to help inform decisions on how to best secure our nation's ports and how to best allocate limited resources to reduce terrorist risks in the maritime environment.[74] Moreover, as we have previously reported, Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness.[75] Conducting an effectiveness assessment that evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks could better position DHS and policymakers in determining the impact of TWIC on enhancing maritime security.

Further, pursuant to executive branch requirements, prior to issuing a new regulation, agencies are to conduct a regulatory analysis, which is to include an assessment of costs, benefits, and associated risks.[76] Prior to

[74] The Coast Guard uses MSRAM to assess risk for various types of vessels and port infrastructure in accordance with the guidance on assessing risk from DHS's National Infrastructure Protection Plan (NIPP). The Coast Guard uses the analysis tool to help implement its strategy and concentrate maritime security activities when and where relative risk is believed to be the greatest. The model assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios; that is, it combines potential targets with different means of attack, as recommended by the risk assessment aspect of the NIPP. Also in accordance with the NIPP, the model is designed to support decision making for the Coast Guard. At the national level, the model's results are used, among other things, for identifying capabilities needed to combat future terrorist threats.

[75] GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).

[76] Office of Management and Budget, Circular A-4, *Regulatory Analysis* (Revised Sept. 17, 2003) provides guidance to federal agencies on the development of regulatory analysis as required by Executive Order 12866 of September 30, 1993, as amended by Executive Order 13258 of February 26, 2002, and Executive Order 13422 of January 18, 2007, "Regulatory Planning and Review." According to Executive Order 12866, agencies should adhere to certain specified principles, such as (1) with respect to setting regulatory priorities, each agency shall consider, to the extent reasonable, the degree and nature of the risks posed by various substances or activities within its jurisdiction, and (2) each agency shall base its decisions on the best reasonably obtainable scientific, technical, economic, and other information concerning the need for, and consequences of, the intended regulation. According to Circular A-4, a regulatory analysis should include the following three basic elements: (1) a statement of the need for the proposed action, (2) an examination of alternative approaches, and (3) an evaluation of the benefits and costs—quantitative and qualitative—of the proposed action and the main alternatives identified by the action. The evaluation of benefits and costs is to be informed by a risk assessment.

issuing the regulation on implementing the use of TWIC as a flashpass, DHS conducted a regulatory analysis, which asserted that TWIC would increase security. The analysis included an evaluation of the costs and benefits related to implementing TWIC. However, DHS did not conduct a risk-informed cost-benefit analysis that considered existing security risks. For example, the analysis did not account for the costs and security risks associated with designing program controls to prevent an individual from acquiring an authentic TWIC using a fraudulent identity and limiting access to secure areas of MTSA-regulated facilities and vessels to those with a legitimate need, in accordance with stated mission needs. As a proposed regulation on the use of TWIC with biometric card readers is under development, DHS is to issue a new regulatory analysis. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and needed corrective actions could better inform and enhance the reliability of the new regulatory analysis. Moreover, these actions could help DHS identify and assess the full costs and benefits of implementing the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks, and help ensure that the TWIC program is more effective and cost-efficient than existing measures or alternatives at enhancing maritime security.

Coast Guard's Approach for Monitoring and Enforcing TWIC Compliance Could Be Improved by Enhancing Its Collection and Assessment of Maritime Security Information

Internal control standards state that (1) internal controls should be designed to ensure that ongoing monitoring occurs in the course of normal operations, and (2) information should be communicated in a form and within a time frame that enables management to carry out its internal control responsibilities.[77] Further, our prior work has stated that Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness.[78] The Coast Guard uses its Marine Information for Safety and Law Enforcement (MISLE) database to meet these needs by recording activities related to MTSA-regulated facility and vessel oversight, including observations of TWIC-related deficiencies.[79] The purpose of MISLE is to provide the capability to collect, maintain, and

[77] See GAO/AIMD-00-21.3.1.

[78] See GAO/GGD-96-118.

[79] MISLE began operating in December 2001 and is the Coast Guard's primary data system for documenting facility oversight and other activities.

retrieve information necessary for the administration, management, and documentation of Coast Guard activities. In February 2008, we reported that flaws in the data in MISLE limit the Coast Guard's ability to accurately portray and appropriately target oversight activities.[80]

In accordance with Coast Guard policy, Coast Guard inspectors are required to verify TWIC cards during annual compliance exams and security spot checks, and may do so in the course of other Coast Guard duties. As part of each inspection, Coast Guard inspectors are, among other things, to: (1) ensure that the card is authentic by examining it to visually verify that it has not been tampered with; (2) verify identity by comparing the photograph on the card with the TWIC holder to ensure a match; (3) check the card's physical security features; and (4) ensure the TWIC is valid—a check of the card's expiration date. Additionally, Coast Guard inspectors are to assess the proficiency of facility and vessel security personnel in complying with TWIC requirements through various means including oral examination, actual observation, and record review. Coast Guard inspectors randomly select workers to check their TWICs during inspections. The number of TWIC cards checked is left to the discretion of the inspectors.

As of December 17, 2010, according to Coast Guard data, 2,135 facilities have undergone at least 2 MTSA inspections as part of annual compliance exams and spot checks. In reviewing the Coast Guard's records of TWIC-related enforcement actions, we found that, in addition to verifying the number of inspections conducted, the Coast Guard is generally positioned to verify that TWIC cards are being checked by Coast Guard inspectors and, of the card checks that are recorded, the number of cardholders who are compliant and noncompliant. For instance, the Coast Guard reported inspecting 129,464 TWIC holders' cards from May 2009 through January 6, 2011. The Coast Guard reported that 124,203 of the TWIC holders, or

[80] We recommended that, among other things, the Coast Guard assess MISLE compliance data, including the completeness of the data, data entry, consistency, and data field problems, and make any changes needed to more effectively use MISLE data. DHS concurred with this recommendation. The Coast Guard acknowledged the need for improvement in MISLE compliance data and has taken initial steps to reduce some of the database concerns identified in our previous work. However, as of January 2011, the recommendation has not been fully addressed. See GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, GAO-08-12 (Washington, D.C.: Feb. 14, 2008).

96 percent, were found to be compliant—possessed a valid TWIC.[81] However, according to Coast Guard officials, local Coast Guard inspectors may not always or consistently record all inspection attempts. Consequently, while Coast Guard officials told us that inspectors verify TWICs as part of all security inspections, the Coast Guard could not reliably provide the number of TWICs checked during each inspection.

Since the national compliance deadline in April 2009 requiring TWIC use at MTSA-regulated facilities and vessels, the Coast Guard has not identified major concerns with TWIC implementation nationally. However, while the Coast Guard uses MISLE to track program compliance, because of limitations in the MISLE system design, the processes involved in the collection, cataloguing, and querying of information cannot be relied upon to produce the management information needed to assess trends in compliance with the TWIC program or associated vulnerabilities. For instance, when inspectors document a TWIC card verification check, the system is set up to record the number of TWICs reviewed for different types of workers and whether the TWIC holders are compliant or noncompliant. However, other details on TWIC-related deficiencies, such as failure to ensure that all facility personnel with security duties are familiar with all relevant aspects of the TWIC program and how to carry them out, are not recorded in the system in a form that allows inspectors or other Coast Guard officials to easily and systematically identify that a deficiency was related to TWIC. For example, from January 2009 through December 2010, the Coast Guard reported issuing 145 enforcement actions as a result of annual compliance exams or security spot checks at the 2,135 facilities that have undergone the inspections.[82] These included 57 letters of warning, 40 notices of violation, 32 civil penalties, and 16 operations controls (suspension or restriction of operations). However, it would be labor-intensive for the Coast Guard to identify how many of the 57 letters of warning or 40 notices of violation were TWIC related, according to a Coast Guard official responsible for TWIC compliance, because there is not an existing query designed to extract this information

[81] These numbers represent a combination of visual and electronic verifications because the TWIC verification window in MISLE is not currently designed to capture whether cards are verified visually or electronically. According to Coast Guard officials, with the recent deployment of handheld readers to Coast Guard units, the Coast Guard is in the process of enhancing MISLE to include the ability to distinguish between the number of visual inspections of cards and the number of verifications conducted using the handheld readers.

[82] According to the Coast Guard, 2,509 facilities are subject to MTSA and must actively implement TWIC provisions.

from the system. Someone would have to manually review each of the 97 inspection reports in the database indicating either a letter of warning or a notice of violation to verify whether or not the deficiencies were TWIC related. As such, the MISLE system is not designed to readily provide information that could help management measure and assess the overall level of compliance with the TWIC program or existing vulnerabilities.

According to a Coast Guard official responsible for TWIC compliance, Coast Guard headquarters staff has not conducted a trend analysis of the deficiencies found during reviews and inspections and there are no other analyses they planned to conduct regarding enforcement until after readers are required to be used. According to the Coast Guard, it can generally identify the number of TWICs checked and recorded in the MISLE system. However, it cannot perform trend analysis of the deficiencies as it would like to do, as it requires additional information. In the interim, as of January 7, 2011, the Coast Guard reported deploying 164 handheld biometric readers nationally to units responsible for conducting inspections.[83] These handheld readers are intended to be the Coast Guard's primary means of TWIC verification. During inspections, Coast Guard inspectors use the card readers to electronically check TWICs in three ways: (1) verification—a biometric one-to-one match of the fingerprint; (2) authentication—electronically confirming that the certificates on the credential are authentic; and (3) validation—electronically check the card against the "hotlist" of invalid or revoked cards. The Coast Guard believes that the use of these readers during inspections will greatly improve the effectiveness of enforcement efforts and enhance record keeping through the use of the readers' logs.

As a result of limitations in MISLE design and the collection and recording of inspection data, it will be difficult for the Coast Guard to identify trends nationwide in TWIC-related compliance, such as whether particular types of facilities or a particular region of the country have greater levels of noncompliance, on an ongoing basis. Coast Guard officials acknowledged these deficiencies and reported that they are in the process of making enhancements to the MISLE database and plan to distribute updated guidance on how to collect and input information into MISLE to the Captains of the Port. However, as of January 2011, the Coast Guard had

[83] The Coast Guard estimated a need for 300 handheld biometric readers, based on an estimate of 5 readers for each of the Coast Guard's major field inspections units across the country.

not yet set a date for implementing these changes. Further, while this is a good first step, these enhancements do not address weaknesses related to the collection process and querying of MISLE information so as to facilitate the Coast Guard performing trend analysis of the deficiencies as part of its compliance reviews. By designing and implementing a cost-effective and practical method for collecting, cataloging, and querying TWIC-related compliance information, the Coast Guard could be better positioned to identify and assess TWIC-related compliance and enforcement trends, and to obtain management information needed to assess and understand existing vulnerabilities with the use of TWIC.

Conclusions

As the TWIC program continues on the path to full implementation—with potentially billions of dollars needed to install TWIC card readers in thousands of the nation's ports, facilities, and vessels at stake—it is important that Congress, program officials, and maritime industry stakeholders fully understand the program's potential benefits and vulnerabilities, as well as the likely costs of addressing these potential vulnerabilities. Identified internal control weaknesses and vulnerabilities include weaknesses in controls related to preventing and detecting identity fraud, assessing the security threat that individuals with extensive criminal histories pose prior to issuing a TWIC, and ensuring that TWIC holders continue to meet program eligibility requirements. Thus, conducting an internal control assessment of the program by analyzing controls, identifying related weaknesses and risks, and determining cost-effective actions to correct or compensate for these weaknesses could better position DHS to provide reasonable assurance that control weaknesses do not impede the program from meeting mission needs.

In addition, conducting an effectiveness assessment could help provide reasonable assurance that the use of TWIC enhances the posture of security beyond efforts already in place or identify the extent to which TWIC may possibly introduce security vulnerabilities because of the way it has been designed and implemented. This assessment, along with the internal controls assessment, could be used to enhance the regulatory analysis to be conducted as part of implementing a regulation on the use of TWIC with readers. More specifically, considering identified security risks and needed corrective actions as part of the regulatory analysis could provide insights on the full costs and benefits of implementing the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks. This is important because, unlike prior access control approaches which allowed access to a specific facility, the TWIC potentially facilitates access to thousands of facilities once the federal

government attests that the TWIC holder has been positively identified and is deemed not to be a security threat. Further, doing so as part of the regulatory analysis could better assure DHS, Congress, and maritime stakeholders that TWIC program security objectives will be met. Finally, by designing and implementing a cost-effective and practical method for collecting, cataloging, and querying TWIC-related compliance information, the Coast Guard could be better positioned to identify trends and to obtain management information needed to assess and understand existing vulnerabilities with the use of TWIC.

Recommendations for Executive Action

To identify effective and cost-efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, we recommend that the Secretary of Homeland Security take the following four actions:

- Perform an internal control assessment of the TWIC program by (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. This assessment should consider weaknesses we identified in this report among other things, and include:
  - strengthening the TWIC program's controls for preventing and detecting identity fraud, such as requiring certain biographic information from applicants and confirming the information to the extent needed to positively identify the individual, or implementing alternative mechanisms to positively identify individuals;
  - defining the term extensive criminal history for use in the adjudication process and ensuring that adjudicators follow a clearly defined and consistently applied process, with clear criteria, in considering the approval or denial of a TWIC for individuals with extensive criminal convictions not defined as permanent or interim disqualifying offenses; and
  - identifying mechanisms for detecting whether TWIC holders continue to meet TWIC disqualifying criminal offense and immigration-related eligibility requirements after TWIC issuance to prevent unqualified individuals from retaining and using authentic TWICs.
- Conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the

posture of security beyond efforts already in place given costs and program risks.

- Use the information from the internal control and effectiveness assessments as the basis for evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks as part of conducting the regulatory analysis on implementing a new regulation on the use of TWIC with biometric card readers.
- Direct the Commandant of the Coast Guard to design effective methods for collecting, cataloguing, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities.

Agency Comments and Our Evaluation

We provided a draft of the sensitive version of this report to the Secretary of Homeland Security for review and comment on March 18, 2011. DHS provided written comments on behalf of the Department, the Transportation Security Administration, and the United States Coast Guard, which are reprinted in full in appendix IV. In commenting on our report, DHS stated that it concurred with our four recommendations and identified actions planned or under way to implement them.

While DHS did not take issue with the results of our work, DHS did provide new details in its response that merit additional discussion. First, DHS noted that it is working to strengthen controls around applicant identity verification in TWIC, but that document fraud is a vulnerability to credential-issuance programs across the federal government, state and local governments, and the private sector. DHS further noted that a governmentwide infrastructure does not exist for information sharing across all entities that issue documents that other programs, such as TWIC, use to positively authenticate an individual's identity. We acknowledge that such a government-wide infrastructure does not exist, and, as discussed in our report, recognize that there are inherent weaknesses in relying on identity documents alone to confirm an individual's identity. However, positively identifying individuals—or confirming their identity—and determining their eligibility for a TWIC is a key stated program goal. Issuing TWICs to individuals without positively identifying them and subsequently assuring their eligibility could, counter to the program's intent, create a security vulnerability. While we recognize that additional costs could be imposed by requiring positive identification checks, taking actions to strengthen the existing identity authentication

process, such as only accepting documents that TSA can and does confirm to be authentic with the issuing agency, and verifying an applicant's business need, could enhance TWIC program efforts to prevent and detect identity fraud and enhance maritime security.

Second, DHS stated that it is working to continually verify TWIC-holder eligibility after issuance but also noted the limitations in the current process. While TSA does receive some criminal history records information when it sends fingerprints to the FBI, the information is not provided recurrently, nor is the information necessarily complete. DHS stated that to provide the most robust recurrent vetting against criminal records, TSA would need access to additional state and federal systems, and have additional authority to do so. As we reported, FBI and TWIC officials stated that because the TWIC background check is considered to be for a noncriminal justice purpose, policy and statutory provisions hamper the program from running the broader FBI fingerprint-based check using the fingerprints collected at enrollment on an ongoing basis. However, we continue to believe that TSA could compensate for this weakness by leveraging existing mechanisms available to maritime stakeholders. For example, other governing entities—such as the Alabama State Port Authority—that have an interest in ensuring the security of the maritime environment, might be willing to establish a mechanism for independently sharing relevant information when warranted. Absent efforts to leverage available information sources, TSA may not be successful in tempering existing limitations.

Lastly, DHS sought clarification on the reporting of our investigators' success at breaching security at ports during covert testing. Specifically, in its comments, DHS noted that it believes that our report's focus on access to port areas rather than access to individual facilities can be misleading. DHS noted that we do not report on the number of facilities that our investigators attempted to gain access to within each port area. DHS stated that presenting the breaches in terms of the number of port areas breached rather than the number of facilities paints a more troublesome picture of the actual breaches that occurred. We understand DHS's concern but continue to believe that the results of our investigators' work, as reported, fairly and accurately represents the results and significance of the work conducted. The goal of the covert testing was to assess whether or not weaknesses exist at ports with varying characteristics across the nation, not to define the pervasiveness of existing weaknesses by type of facility, volume, or other characteristic. Given the numerous differences across facilities and the lack of publicly available information and related statistics for each of the approximately 2,509 MTSA-regulated facilities, we

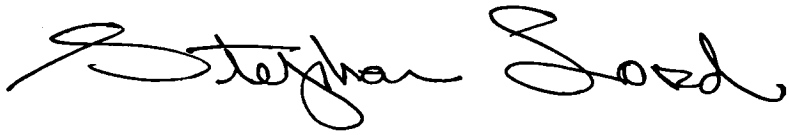
identified covert testing at the port level to be the proper unit of analysis for our review and reporting purposes. Conducting a detailed assessment of the pervasiveness of existing weaknesses by type of facility, volume, or other characteristics as suggested by DHS would be a more appropriate tasking for the Coast Guard as part of its continuing effort to ensure compliance with TWIC-related regulations.

In addition, with regard to covert testing, DHS further commented that the report does not distinguish among breaches in security using a counterfeit TWIC or an authentic TWIC card obtained with fraudulent documents. DHS noted that because there is no "granularity" with the report as to when a specific card was used, one can be left with the unsupported impression that individual facilities in all cases were failing to implement TWIC visual inspection requirements. For the above noted reason, we did not report on the results of covert testing at the facility level. However, our records show that use of counterfeit TWICs was successful for gaining access to more than one port where our investigators breached security. Our investigators further report that security officers never questioned the authenticity of TWICs presented for acquiring access. Our records show that operations at the locations our investigators breached included cargo, containers, and fuel, among others.

In addition, TSA provided written technical comments, which we incorporated into the report, as appropriate.

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, 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 about this report, please contact me at (202) 512-4379 or 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.



Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Requesters

The Honorable John D. Rockefeller, IV
Chairman
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable John L. Mica
Chairman
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Frank R. Lautenberg
Chairman
Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Olympia J. Snowe
Ranking Member
Subcommittee on Oceans, Atmosphere, Fisheries, and Coast Guard
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Frank A. LoBiondo
Chairman
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Mike Rogers
Chairman
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

The Honorable Candice S. Miller
Chairwoman
Subcommittee on Border and Maritime Security
Committee on Homeland Security
House of Representatives

Appendix I: Key Steps in the TWIC Enrollment Process

Transportation workers are enrolled by providing biographic information, such as name, date of birth, and address, and proof of identity documents, and then photographed and fingerprinted at 1 of approximately 149 enrollment centers by trusted agents. A trusted agent is a member of the TWIC team who has been authorized by the federal government to enroll transportation workers in the TWIC program and issue TWIC cards. Trusted agents are subcontractor staff acquired by Lockheed Martin as part of its support contract with TSA for the TWIC program. Table 2 below summarizes key steps in the enrollment process.

Table 2: TWIC Enrollment Process Summary

1.	The TWIC applicant fills out a TWIC Application and Disclosure Form and affirms that the information he or she is providing to TSA is truthful.
2.	The applicant is required to present documentation to establish his or her identity to the trusted agent at the enrollment center. The documentation required is dependant upon the applicant's legal presence in the United States or whether the applicant was born in the United States.
3.	The trusted agent (government contractor) captures the applicant's biographic information, such as name and date of birth, in the TWIC system. This can be done in various ways, such as by scanning fingerprints and certain identity documents or by manually typing information into the system.
4.	The trusted agent reviews the identity documents to establish and confirm the applicant's identity and to confirm the documents' authenticity by reviewing the physical security features on the documents.
5.	The trusted agent scans the identity documents to record a digital image of the applicant's identity information.
6.	The trusted agent uses a machine-readable document scanning device to assess the risk of certain documents being fraudulent. Not all documents can be assessed using this device.
7.	The applicant's 10 fingerprints (where available) are captured in the system. The presence of nonsuitable fingerprints or lack of a finger for biometric use is documented in the system by the trusted agent.
8.	The applicant's digital picture is taken.
9.	The enrollment record is completed, encrypted, and is forwarded by the trusted agent to undergo the TWIC program's background checking procedures.

Source: GAO analysis of the TWIC program enrollment process and documentation.

Appendix II: TWIC Program Funding

According to TSA and Federal Emergency Management Agency (FEMA) program officials, from fiscal year 2002 through 2010, the TWIC program had funding authority totaling $420 million. Through fiscal year 2009, $111.5 million in appropriated funds, including reprogramming and adjustments, had been provided to TWIC (see table 3 below). An additional $196.8 million in funding was authorized from fiscal years 2008 through 2010 through the collection of TWIC enrollment fees by TSA, and $111.7 million had been made available to maritime facilities implementing TWIC from FEMA grant programs—the Port Security Grant Program and the Transit Security Grant Program—from fiscal years 2006 through 2010. In addition, industry has spent between approximately $185.7 million and $234 million to purchase 1,765,110 TWICs as of January 6, 2011.[1] The costs for implementing the TWIC program, as estimated by TSA for informing the regulation on requiring the use of TWIC as an identification credential, is from $694.3 million to $3.2 billion over a 10-year period. This estimate includes the costs related to purchasing TWICs and visually inspecting them. However, this estimate does not include the costs related to implementing TWIC with biometric card readers or related access control systems.[2]

[1] Range based on a reduced fee of $105.25 per TWIC for workers with current, comparable background checks or a $132.50 fee per TWIC for those without.

[2] See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule, 72 Fed. Reg. 3492, 3571 (2007).

Table 3: TWIC Program Funding from Fiscal Years 2002 through 2010

Dollars in millions

Fiscal year	Appropriated	Reprogramming	Adjustments	TWIC fee authority[a]	Federal security grant awards related to TWIC[b]	Total funding authority
2002	0	0	0	0	0	0
2003	$5.0	0	$20	0	0	$25.0
2004	$49.7	0	0	0	0	$49.7
2005	$5.0	0	0	0	0	$5.0
2006	0	$15.0	0	0	$24.3	$39.3
2007	0	$4.0	$4.7	0	$31.5[c]	$40.2
2008	$8.1	0	0	$42.5	$18.0	$68.6
2009	0	0	0	$109.3	$22.2[d]	$131.5
2010	0	0	0	$45.0	$15.7	$60.7
Total	**$67.8**	**$19.0**	**$24.7**	**$196.8**	**$111.7**	**$420**

Source: GAO analysis of TWIC program funding reported by TSA and FEMA.

[a]Figures in the TWIC fee authority column represent the dollar amount TSA is authorized to collect from TWIC enrollment fees and not the actual dollars collected. TSA reports to have collected $41.7 million for fiscal year 2008, $76.2 million for fiscal year 2009, and $30.6 million for fiscal year 2010.

[b]According to FEMA, many of these awards are issued as cooperative agreements and, as such, the scope and amounts may change as the project(s) proceed. Also, FEMA has not received projects from all grant recipients so the total number of projects may increase slightly over time.

[c]Federal security grant funding subtotal for fiscal year 2007 includes $19.2 million in fiscal year Port Security Grant Program funding, $10.8 million in supplemental funding, and $1.5 million in Transit Security Grant Program funding.

[d]Federal security grant funding subtotal for fiscal year 2009 includes $3.9 million in fiscal year Port Security Grant Program funding and an additional $18.3 million in American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5, 123 Stat. 115 (2009)) funding.

Appendix III: List of Documents U.S.-Born Citizens or Nationals Must Select from to Present When Applying for a TWIC

TWIC applicants who are citizens of the United States (or its outlying possessions) and were born inside the United States (or its outlying possessions), must provide one document from list A or two documents from list B. If two documents from list B are presented, at least one of them must be a government-issued photo identification, such as a state-issued driver's license, military ID card, or state identification card.

List A

- Unexpired United States passport book or passport card
- Unexpired Merchant Mariner Document
- Unexpired Free and Secure Trade Card[1]
- Unexpired NEXUS Card[2]
- Unexpired Secure Electronic Network for Travelers Rapid Inspection Card

List B

- Unexpired driver's license issued by a state or outlying possession of the United States
- Unexpired identification card issued by a state or outlying possession of the United States. Must include a state or state agency seal or logo (such as state port authority identification or state university identification)
- Original or certified copy of birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal
- Voter's registration card
- United States military identification card or United States retired military identification
- United States military dependent's card
- Expired United States passport (within 12 months of expiration)
- Native American tribal document (with photo)
- United States Social Security card
- United States military discharge papers (DD-214)
- Department of Transportation medical card
- United States civil marriage certificate

[1] The Free and Secure Trade (FAST) Card is to be issued to approved commercial drivers to facilitate the travel of low-risk screened shipments across the borders between the U.S.-Canadian border and to the U.S. from Mexico.

[2] The NEXUS card can be used as an alternative to the passport for air, land, and sea travel into the United States for U.S. and Canadian citizens. The NEXUS program allows prescreened travelers expedited processing by United States and Canadian officials at dedicated processing lanes at designated northern border ports of entry, at NEXUS kiosks at Canadian Preclearance airports, and at marine reporting locations.

- Unexpired Merchant Mariner License bearing an official raised seal, or a certified copy
- Unexpired Department of Homeland Security/Transportation Security Administration Transportation Worker Identification Credential Card
- Unexpired Merchant Mariner Credential

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

Listed below are criminal offenses that can prevent TWIC applicants from being issued a TWIC. Pursuant to TSA implementing regulations, permanent disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(a). Permanent disqualifying offenses that can be waived are those offenses defined in 49 C.F.R. 1572.103(a) for which a waiver can be granted in accordance with 49 C.F.R. 1515.7(a)(i). Interim disqualifying offenses are offenses defined in 49 C.F.R. 1572.103(b) for which the applicant has either been (1) convicted, or found not guilty by reason of insanity, within a 7-year period preceding the TWIC application, or (2) incarcerated for within a 5-year period preceding the TWIC application. Applicants with certain permanent criminal offenses and all interim disqualifying criminal offenses may request a waiver of their disqualification. In general, TSA may issue such a waiver and grant a TWIC 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.
4. 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 transportations 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).

The interim disqualifying felonies.

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 CFR § 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.
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 felonies.

Appendix V: Comparison of Authentic and Counterfeit TWICs

Figure 1: Comparison of Authentic and Counterfeit TWICs

Details from this section were removed because the agency deemed them to be sensitive security information.

Appendix VI: Comments from the Department of Homeland Security

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

Homeland Security

May 5, 2011

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

Dear Mr. Lord:

Re: GAO-11-657, Draft Report, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives*

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.

Transportation Worker Identification Credential (TWIC) is a vital security program that is jointly administered by the U.S. Coast Guard (USCG) and the Transportation Security Administration (TSA). TSA is responsible for enrollment, vetting, and card production, with the support of the U.S. Citizenship and Immigration Services, while the USCG governs access control requirements and has primary responsibility for enforcement. As of March 2011, TSA has enrolled and vetted more than 1.8 million maritime workers. As a result of DHS's rigorous vetting process, 35,661 individuals were denied from receiving a TWIC. DHS agrees that more work is needed to strengthen existing security controls and has begun efforts to address many of the GAO's findings.

DHS Increasing Applicant Identity Verification Controls

DHS is working to strengthen controls around applicant identity verification in TWIC, knowing that document fraud is a vulnerability to credential-issuance programs across federal, state, and local governments, and the private sector. To establish identity and proof-of-citizenship, TWIC leverages documents issued by multiple federal, state, and local entities. However, a government-wide infrastructure does not exist for information sharing across all entities that issue the breeder documents that relying parties use to positively authenticate an identity. TWIC follows best practices to mitigate the risks from not having visibility or control of the physical characteristics or the issuance process for these documents. Specifically, TWIC uses document authentication readers and requires fraudulent document training of its Trusted Agents as safeguards against document fraud.

1

TWIC will benefit from national efforts to strengthen identity documents. For example, DHS continues to work with the states to implement the requirements of the REAL ID Act for more secure driver's licenses, as well as the underlying issuance processes and procedures. Furthermore, efforts are underway in the Federal Government, state vital records agencies, and departments of motor vehicles to enhance security related to core breeder documents, such as birth certificates, which would assist in positive authentication.

TSA is also actively engaged with the DHS's United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program to include TWIC applicant data into the US-VISIT database, referred to as IDENT. Biometrics placed in IDENT are linked to specific biographic information, enabling a person's identity to be established and then verified by the U.S. Government.

TWIC is also strengthening safeguards against cards being misused after issuance. An upcoming USCG rulemaking will include a requirement for electronic verification of the TWIC card through use of card readers. The use of electronic readers will provide the port or facility authority in charge of access control decisions with a higher level of assurance that the TWIC presented is authentic, valid (not revoked), and unexpired.

DHS Working to Continually Verify TWIC Holder Eligibility after Issuance

DHS strongly agrees on the value of recurrent vetting. DHS is making progress in the effort to reasonably assure that TWIC holders have maintained their eligibility once issued their TWICs. TSA conducts recurrent checks of TWIC holders against the Terrorist Screening Database and other databases. TSA has the authority to revoke TWICs based on the results of recurrent vetting, and use of card readers for electronic verification will strengthen the effectiveness of these processes.

In order to provide the most robust recurrent vetting against criminal history records, TSA needs full access to Criminal History Records Information (CHRI), similar to that of a criminal justice agency or law enforcement officer; this information is available at the state level and accessed via the Interstate Identification Index managed by the U.S. Department of Justice, Federal Bureau of Investigation (FBI). Although TSA receives some CHRI when it sends fingerprints to the FBI for initial vetting, the FBI does not perform recurrent vetting of CHRI on behalf of TSA. The FBI has deemed that TSA's security threat assessments for TWIC are non-criminal justice activities. As a result, TSA is unable to request subsequent CHRI for recurrent vetting without a submission of new fingerprints from the individual. Additionally, TSA may not always receive all available information because of the FBI's designation as 'non-criminal justice' purposes for TSA security threat assessments. States may not upload all available information into the FBI biometric system and may not respond to CHRI requests for "non-criminal justice" activities. DHS has and will continue to work with the FBI and states to try to expand access to the CHRI.

While not a final solution to the challenge of recurrent criminal vetting, including TWIC data in IDENT would provide a framework to initiate more recurrent vetting on CHRI, where available, for TWIC holders. In addition to supporting identity verification, biometric data

2

from IDENT is used to conduct vetting against criminals and immigration violators. TSA and US-VISIT are working to include TWIC data in the IDENT database.

DHS Clarification on GAO Breaches of MTSA-Regulated Ports

DHS would also like to address aspects of GAO's covert operation defined in the report that we believe warrant further clarification.

DHS believes that the focus on access to port areas rather than access to individual facilities can be misleading. Specifically, the report states that GAO investigators successfully penetrated ports between August 2009 and February 2010. However, the report does not breakdown the number of facilities to which GAO attempted to gain access within each port area. Each port is unique in design and operation—ranging from some ports housing hundreds of individual facilities spread over a large geographic area to other ports containing only a few facilities in a small geographic area with one main access control point. While GAO stated that it did not require its covert investigators to record the individual attempts to access facilities, investigators indicated during discussions with USCG that they were successful in gaining unauthorized access at some individual facilities within the port areas. The presentation of breaches at port versus individual facilities paints a more troublesome picture of the actual breaches that occurred.

Third, the report does not distinguish among fraud committed with counterfeit TWIC cards, authentic TWIC cards obtained with fraudulent documents, and access control decisions made by facility personnel. Each type of fraud has a different mitigation technique. The fact that a Facility Security Officer does not question what appears to be a valid card should not be intertwined with cases in which a counterfeit card was presented to gain access. Because there is no granularity within the report as to when a specific card was used, one can be left with the unsupported impression that individual facilities in all cases were failing to implement TWIC visual inspection requirements. Or, as written in this report, that ports failed to properly implement these requirements.

Recent Developments

The GAO audit was beneficial in helping DHS identify immediate actions that could strengthen the effectiveness of the TWIC program.

TSA has already taken steps to remedy some of the missing internal controls that GAO has identified. Starting in January 2011, the TWIC program initiated a 100-percent review of all fingerprint matches received in the system. These matches could highlight potential fraud in the TWIC enrollment process where one individual could be attempting to enroll under a different identity and possibly with fraudulent documents. During this process, the TWIC program has already referred numerous cases to our Law Enforcement Investigations Unit where investigations are under way.

On February 14, 2011, USCG Headquarters published additional guidance to field units regarding the importance of TWIC inspections and verifications. The guidance directed Captains of the Port to place a higher priority on the review and validation of TWIC verification procedures during the required Maritime Transportation Security Act (MTSA) security inspections. Additionally, the guidance encouraged Captains of the Port and the

3

Facility Security Officers to take advantage of training aids regarding the identification of fraudulent TWICs published on Homeport—the USCG's Internet site for maritime information.

As previously mentioned, the USCG is currently developing an upcoming rulemaking that will include a requirement for card readers at ports and facilities. The TWIC program has completed a pilot that evaluated using card readers for electronic verification of the TWIC card. DHS believes that electronic verification of TWIC cards will significantly enhance protection against counterfeit, tampered, or expired TWIC cards being used to gain access to secure facilities.

TSA is in the initial phases of a modernization effort for its vetting infrastructure. This effort is aimed at consolidating systematic processes related to conducting background checks with the goal of improving the overall security and consistency of our enrollment and vetting processes. As the modernization effort moves forward, the TWIC program will continue to be heavily involved to ensure that any internal control gaps or risks are addressed or further mitigated.

GAO Recommendations

DHS takes the findings of this review very seriously. DHS strongly believes that TWIC has an overall effect of strengthening the security of our Nation's ports. We also acknowledge and appreciate GAO's work to identify opportunities to enhance current program controls. We recognize that breaches did occur and that the Department and port facility owners and operators need to take steps to enhance security. DHS appreciates the opportunity to provide GAO with comments to its audit recommendations.

"To identify effective and cost efficient methods for meeting TWIC program objectives, and assist in determining whether the benefits of continuing to implement and operate the TWIC program in its present form and planned use with readers surpass the costs, we recommend that the Secretary of Homeland Security take the following four actions:

Recommendation 1: Perform an internal control assessment of the TWIC program by (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. This assessment should consider weaknesses we identified in this report, among other things, and include:

- strengthening the TWIC program's controls for preventing and detecting identity fraud, such as requiring certain biographic information from applicants and confirming the information to the extent needed to positively identify the individual, or implementing alternative mechanisms to positively identify individuals;

- defining the term extensive criminal history for use in the adjudication process and ensuring that adjudicators follow a clearly defined and consistently applied process, with clear criteria, in considering the approval and denial of a TWIC for individuals with extensive criminal convictions not defined as a permanent or interim disqualifying offense: and

4

- identifying mechanisms for detecting whether TWIC-holders continue to meet TWIC disqualifying criminal offense and immigration-related eligibility requirements after TWIC issuance to prevent unqualified individuals from retaining and using authentic TWICs."

Response: Concur. DHS agrees that an internal control assessment should and will be performed. Once the final GAO report is issued, DHS will initiate a comprehensive review of current internal controls with a specific focus on the controls highlighted in this report. In the interim, TSA and USCG are evaluating and implementing new internal controls as discussed in this letter.

Recommendation 2: "Conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluates whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks."

Response: Concur. DHS agrees that the results of the internal control assessment should be used to further evaluate the effectiveness of the TWIC program.

Recommendation 3: "Use the information from the internal control and effectiveness assessments as the basis for the evaluating the costs, benefits, security risks, and corrective actions needed to implement the TWIC program in a manner that will meet stated mission needs and mitigate existing security risks as part of conducting the regulatory analysis on implementing a new regulation on the use of TWIC with biometric card readers."

Response: Concur. As the internal control assessments progress, any applicable data or risks will be communicated to USCG for consideration during their regulatory analysis.

Recommendation 4: "Direct the Commandant of the Coast Guard to design effective methods for collecting, cataloguing, and querying TWIC-related compliance issues to provide the Coast Guard with the enforcement information needed to assess trends in compliance with the TWIC program and identify associated vulnerabilities."

Response: Concur. USCG has already incorporated changes to its current version of Marine Information for Safety and Law Enforcement (MISLE) to enhance data collection since the TWIC compliance date of April 15, 2009. Incorporation of additional changes is planned in a future release of MISLE that will add to current capabilities to collect data and allow for more detailed trend analysis.

Again, thank you for the opportunity to review and comment on this draft report. We look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

5

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, David Bruno (Assistant Director), Joseph P. Cruz, Scott Fletcher, Geoffrey Hamilton, Richard Hung, Lemuel Jackson, Linda Miller, Jessica Orr, and Julie E. Silvers made key contributions to this report.