United States Government Accountability

GAO

Testimony

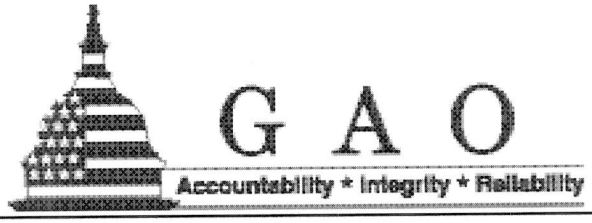
Before the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Tuesday, May 10, 2011

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

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

Statement of Stephen M. Lord, Director
Homeland Security and Justice Issues



Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee:

I am pleased to be here today to discuss credentialing issues associated with the security of U.S. transportation systems and facilities. Securing these systems requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and international commerce. 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 (MTSA) required regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they possess a biometric transportation security card and are authorized to be in such an area. MTSA further required that biometric transportation security cards be issued to eligible individuals unless determined that an applicant poses a security risk warranting denial of the card. The Transportation Worker Identification Credential (TWIC)

[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).

program is designed to implement these biometric maritime security card requirements.[2]

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

[2]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 vessels. 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. Biometrics refers to technologies that measure and analyze human body characteristics for authentication purposes. The Department of Homeland Security (DHS) has 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 do not include costs associated with implementing and operating readers. A pilot on the use of TWIC with card readers is currently underway and will inform a proposed TWIC regulation, and these figures are to be updated as part of this process.

unescorted access to secure areas of the nation's transportation system and immediately revoke the individual's permissions.

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. In addition, DHS's Screening Coordination Office facilitates coordination among the various DHS components involved in TWIC.

My statement is based on a report we are releasing publicly today on the TWIC program.[3] Like the report, it will discuss the extent to which: (1) TWIC processes for enrollment, background checking, and use are designed to provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to qualified individuals, and (2) DHS has assessed the effectiveness of TWIC, and whether the Coast Guard has effective systems in place to measure compliance.

For the report, we reviewed applicable laws, regulations, and policies, as well as documentation provided by TSA on the TWIC program systems and processes. We also reviewed the processes and data sources with TWIC program management from TSA and Lockheed Martin (the contractor responsible for implementing the program) and met with officials from TSA and the Coast Guard, as well as the Criminal Justice Information Services Division at the Federal Bureau of Investigation (FBI). We then evaluated the processes against the TWIC program's mission needs and *Standards for Internal Control in the Federal Government*.[4] Further, our investigators conducted

[3]See GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

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

covert testing at enrollment center(s) to identify whether individuals providing fraudulent information could acquire an authentic TWIC, and at maritime ports with MTSA-regulated facilities and vessels to identify security vulnerabilities and program control deficiencies. In addition, we reviewed the type and substance of management information available to the Coast Guard and compared them to Standards for Internal Control in the Federal Government. We conducted this work in accordance with generally accepted government auditing standards. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

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 meet the program's stated mission needs or provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals. Specifically, internal controls[5] 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 purpose, TSA's focus in designing the TWIC program was on facilitating the

[5]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.

issuance of TWICs to maritime workers. However, TSA did not assess the internal controls in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals. For example, controls that the TWIC program has in place to identify the use of potentially counterfeit identity documents are not used to routinely inform background checking processes. Additionally, controls are not in place to determine whether an applicant has a need for a TWIC. For example, 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, among other things. However, TSA enrollment processes do not require that this information be provided by applicants.

In addition, TWIC program controls are not designed to require that adjudicators 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.[6] For example, 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. These offenses might not

[6]Threat assessment processes for the TWIC program include conducting background checks to determine whether each TWIC applicant poses a security threat. 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 who TSA determines or suspects of posing a threat to national security, to transportation security, or of terrorism.

permanently disqualify an individual from obtaining a TWIC if TSA determines that an applicant does not represent a security threat. 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. Although TSA has the discretion and authority to consider the totality of an individual's criminal record, including the existence of (1) extensive criminal convictions, (2) criminal offenses not defined as a permanent or interim disqualifying criminal offense, such as theft or larceny, and (3) certain 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 commenting on our report, DHS concurred with our related recommendation, and consequently may address this weakness as part of its efforts to correct internal control weaknesses in the TWIC program.

Further, TWIC program controls are not designed to provide reasonable assurance that TWIC holders have maintained their eligibility once issued TWICs. For example, controls are not designed to determine whether TWIC holders have committed disqualifying crimes at the federal or state level after being granted a TWIC. Although existing policies may hamper TSA's ability to check FBI-held fingerprint-based criminal history records for the TWIC program on an ongoing basis after TWIC issuance, 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. In addition, controls are not designed to provide reasonable assurance that TWIC holders continue to meet immigration status eligibility requirements. For example, 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 it has 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.[7]

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. During these tests at several selected ports, our 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). Our investigators did not gain unescorted access to a port where a secondary port-specific identification was required in addition to the TWIC. TSA and Coast Guard officials stated that the TWIC card alone is not sufficient and that the cardholder is also required to present a business case. However, our covert tests demonstrated that having an authentic TWIC and a legitimate business case were not always required in practice.

[7]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. 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.

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 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, as we noted in our report, officials did not provide (1) documentation to support their cost concerns and (2) did not complete an assessment of whether they needed to implement additional compensating controls or of the risks associated with not correcting for existing internal control weaknesses. In our May 2011 report, we recommended that the Secretary of Homeland Security 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. DHS officials concurred with our recommendation.

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

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.[8] However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned with card 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. However, internal control weaknesses raise questions about the effectiveness of the TWIC program. 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. Therefore, we recommended in our May 2011 report that the Secretary of Homeland Security 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

[8] 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).

in place given costs and program risks. DHS concurred with our recommendation.

Further, executive branch requirements provide that prior to issuing a new regulation, agencies are to conduct a regulatory analysis, which is to include an assessment of costs, benefits, and risks. Therefore, DHS is required to issue a new regulatory analysis for its proposed regulation on the use of TWIC with biometric card readers. Conducting a regulatory analysis using the information from the internal control and effectiveness assessments could better inform the new regulatory analysis and could help DHS identify and assess the full costs and benefits of implementing the TWIC program. Therefore, in our May 2011 report, we recommended that the Secretary of Homeland Security 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. This should be done in a manner that will meet stated mission needs and mitigate existing security risks as part of the regulatory analysis being completed for the new TWIC biometric card reader regulation. DHS concurred with our recommendation.

Finally, the 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. The Coast Guard uses its Marine Information for Safety and Law Enforcement (MISLE) database to monitor activities related to MTSA-regulated facility and vessel oversight, including observations of TWIC-related deficiencies. Coast Guard officials reported that they are making enhancements to the MISLE database and plan to distribute updated guidance on how to collect and input information.

However, as of May 2011, the Coast Guard had not yet set a date for implementing these changes. Further, these enhancements do not address all weaknesses identified in our report that hamper the Coast Guard's efforts to conduct trend analysis of the deficiencies as part of its compliance reviews. Therefore, in our May 2011 report, we recommended that the Secretary of Homeland Security 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. DHS concurred with our recommendation.

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. The report we are releasing today aims to help inform stakeholder views on these issues.

Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee, this concludes my prepared testimony. I look forward to answering any questions that you may have.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548