



May 2013

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed

GAO Highlights

Highlights of [GAO-13-198](#), a report to congressional committees

Why GAO Did This Study

Within DHS, TSA and USCG manage the TWIC program, which requires maritime workers to complete background checks and obtain biometric identification cards to gain unescorted access to secure areas of Maritime Transportation Security Act (MTSA)-regulated entities. TSA conducted a pilot program to test the use of TWICs with biometric card readers in part to inform the development of a regulation on using TWICs with card readers. As required by law, DHS reported its findings on the pilot to Congress on February 27, 2012. The Coast Guard Authorization Act of 2010 required that GAO assess DHS's reported findings and recommendations. Thus, GAO assessed the extent to which the results from the TWIC pilot were sufficiently complete, accurate, and reliable for informing Congress and the proposed TWIC card reader rule. GAO reviewed pilot test plans, results, and methods used to collect and analyze pilot data since August 2008, compared the pilot data with the pilot report DHS submitted to Congress, and conducted covert tests at four U.S. ports chosen for their geographic locations. The test's results are not generalizable, but provide insights.

What GAO Recommends

Congress should halt DHS's efforts to promulgate a final regulation until the successful completion of a security assessment of the effectiveness of using TWIC. In addition, GAO revised the report based on the March 22, 2013, issuance of the TWIC card reader notice of proposed rulemaking.

View [GAO-13-198](#). For more information, contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov.

May 2013

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed

What GAO Found

GAO's review of the pilot test aimed at assessing the technology and operational impact of using the Transportation Security Administration's (TSA) Transportation Worker Identification Credential (TWIC) with card readers showed that the test's results were incomplete, inaccurate, and unreliable for informing Congress and for developing a regulation (rule) about the readers. Challenges related to pilot planning, data collection, and reporting affected the completeness, accuracy, and reliability of the results. These issues call into question the program's premise and effectiveness in enhancing security.

Planning. The Department of Homeland Security (DHS) did not correct planning shortfalls that GAO identified in November 2009. GAO determined that these weaknesses presented a challenge in ensuring that the pilot would yield information needed to inform Congress and the regulation aimed at defining how TWICs are to be used with biometric card readers (card reader rule). GAO recommended that DHS components implementing the pilot—TSA and the U.S. Coast Guard (USCG)—develop an evaluation plan to guide the remainder of the pilot and identify how it would compensate for areas where the TWIC reader pilot would not provide the information needed. DHS agreed and took initial steps, but did not develop an evaluation plan, as GAO recommended.

Data collection. Pilot data collection and reporting weaknesses include:

- Installed TWIC readers and access control systems could not collect required data, including reasons for errors, on TWIC reader use, and TSA and the independent test agent (responsible for planning, evaluating, and reporting on all test events) did not employ effective compensating data collection measures, such as manually recording reasons for errors in reading TWICs.
- TSA and the independent test agent did not record clear baseline data for comparing operational performance at access points with TWIC readers.
- TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.
- Pilot participants did not document instances of denied access.

TSA officials said challenges, such as readers incapable of recording needed data, prevented them from collecting complete and consistent pilot data. Thus, TSA could not determine whether operational problems encountered at pilot sites were due to TWIC cards, readers, or users, or a combination of all three.

Issues with DHS's report to Congress and validity of TWIC security premise. DHS's report to Congress documented findings and lessons learned, but its reported findings were not always supported by the pilot data, or were based on incomplete or unreliable data, thus limiting the report's usefulness in informing Congress about the results of the TWIC reader pilot. For example, reported entry times into facilities were not based on data collected at pilot sites as intended. Further, the report concluded that TWIC cards and readers provide a critical layer of port security, but data were not collected to support this conclusion. For example, DHS's assumption that the lack of a common credential could leave facilities open to a security breach with falsified credentials has not been validated. Eleven years after initiation, DHS has not demonstrated how, if at all, TWIC will improve maritime security.

Contents

Letter		1
	Background	6
	TWIC Reader Pilot Results Are Not Sufficiently Complete, Accurate, and Reliable for Informing Congress and the TWIC Card Reader Rule	13
	Conclusions	42
	Matter for Congressional Consideration	43
	Agency Comments and Our Evaluation	43
Appendix I	Objective, Scope, and Methodology	48
Appendix II	Key TWIC Implementation Actions	58
Appendix III	TWIC Program Funding	59
Appendix IV	TWIC Reader Pilot Sites, Locations, and Types of Maritime Operation or Industry Group	61
Appendix V	Comments from the Department of Homeland Security	62
Appendix VI	GAO Contact and Staff Acknowledgments	67
Tables		
	Table 1: Three Assessments Planned for the Transportation Worker Identification Credential (TWIC) Reader Pilot	11
	Table 2: Weaknesses in the Transportation Worker Identification Credential (TWIC) Reader Pilot Affecting the Completeness, Accuracy, and Reliability of Data Collected	19
	Table 3: Key Transportation Worker Identification Credential (TWIC) Program Laws and Implementation Actions from November 2002 through November 2012	58

Table 4: Transportation Worker Identification Credential (TWIC)
Program Funding from Fiscal Years 2002 through 2012

Abbreviations

ATSA	Aviation and Transportation Security Act
DHS	Department of Homeland Security
DOD	Department of Defense
EOA	early operational assessment
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
ICE	initial capability evaluation
ITT	initial technical testing
MSRAM	Maritime Security Risk Analysis Model
MTSA	Maritime Transportation Security Act of 2002
NAVAIR	Naval Air Systems Command
NPRM	Notice of Proposed Rulemaking
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	U.S. Coast Guard
SAFE Port Act	Security and Accountability For Every Port Act of 2006
SOVT	Systems Operational Verification Testing
SPAWAR	Space and Naval Warfare Systems Command
ST&E	system test and evaluation
TEMP	Test and Evaluation Master Plan

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



May 8, 2013

Congressional Committees

Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have serious consequences. Maritime workers, including longshoremen, mechanics, truck drivers, and merchant mariners, access secure areas of the nation's estimated 16,400 maritime-related transportation facilities and vessels, such as cargo container and cruise ship terminals, each day while performing their jobs.¹ Securing transportation systems and maritime-related facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and 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.²

The Department of Homeland Security's (DHS) Transportation Worker Identification Credential (TWIC) program was initiated in December 2001 in response to the September 11, 2001, terrorist attacks. The TWIC program is intended to provide a tamper-resistant biometric credential³ to maritime workers who require unescorted access to secure areas of facilities and vessels regulated under the Maritime Transportation

¹For the purposes of this report, the term "maritime-related transportation facilities" refers to seaports, inland ports, offshore facilities, and facilities located on the grounds of ports.

²See, for example, 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); *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); and *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, [GAO-05-106](#) (Washington, D.C.: Dec. 10, 2004).

³A biometric access control system consists of technology that determines an individual's identity by detecting and matching unique physical or behavioral characteristics, such as fingerprint or voice patterns, as a means of verifying personal identity.

Security Act of 2002 (MTSA).⁴ TWIC is to enhance the ability of MTSA-regulated facility and vessel owners and operators to control access to their facilities and verify workers' identities. Under current statute and regulation, maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities or vessels are required to obtain a TWIC,⁵ and facility and vessel operators are required by regulation to visually inspect each worker's TWIC before granting unescorted access.⁶ Prior to being granted a TWIC, maritime workers are required to undergo a background check, known as a security threat assessment.

Within DHS, the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) jointly administer the TWIC program. TSA is responsible for enrollment, security threat assessments, and TWIC enrollee data systems operations and maintenance. USCG is responsible for the enforcement of regulations governing the use of TWICs at MTSA-regulated facilities and vessels. In addition, DHS's Screening Coordination Office facilitates coordination among the various DHS components involved in TWIC, such as TSA and USCG.⁷ As of November 2012, TSA operates approximately 135 centers where workers can enroll in the program and pick up their TWIC cards. These centers are located in ports and in areas where there are concentrations of maritime activity throughout the United States and its territories. As of April 11, 2013, TSA has issued nearly 2.3 million TWICs.

⁴Pub. L. No. 107-295, 116 Stat. 2064. According to Coast Guard regulations, a secure area is an area that has security measures in place for access control. 33 C.F.R. § 101.105. For most maritime facilities, the secure area is generally any place inside the outermost access control point. For a vessel or outer continental shelf facility, such as offshore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. A restricted area is a part of a secure area that needs more limited access and higher security. Under Coast Guard regulations, an owner/operator must designate certain specified types of areas as restricted. For example, storage areas for cargo are restricted areas under Coast Guard regulations. 33 C.F.R. § 105.260(b)(7).

⁵46 U.S.C. § 70105(a); 33 C.F.R. § 101.514.

⁶33 C.F.R. §§ 104.265(c), 105.255(c).

⁷DHS's Screening Coordination Office was established in 2006 to coordinate and harmonize the numerous and disparate credentialing and screening initiatives within DHS.

We have been reporting on TWIC progress and challenges since September 2003.⁸ Among other issues, we highlighted steps that TSA and USCG were taking to meet an expected surge in initial enrollment as well as various challenges experienced in the TWIC testing conducted by a contractor for TSA and USCG from August 2004 through June 2005. We also identified challenges related to ensuring that the TWIC technology works effectively in the harsh maritime environment.⁹ In November 2009, we reported on the design and approach of a pilot initiated in August 2008 to test TWIC readers, and found that DHS did not have a sound evaluation methodology to ensure information collected through the TWIC reader pilot would be complete and accurate.¹⁰ Moreover, in May 2011, we reported that 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.¹¹ Additional information on our past work and related recommendations is discussed later in this report.

USCG is leading efforts to develop a new TWIC regulation (rule) regarding the use of TWIC cards with readers (known as the TWIC card reader rule). The TWIC card reader rule is expected to define if and under what circumstances facility and vessel owners and operators are to use electronic card readers to verify that a TWIC card is valid. To help inform this rulemaking and to fulfill the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) requirement, TSA conducted a TWIC reader pilot from August 2008 through May 2011 to test a variety of biometric readers, as well as the credential authentication and validation process.¹² The TWIC reader pilot, implemented with the voluntary participation of maritime port, facility, and vessel operators, was to test

⁸GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, [GAO-03-1155T](#) (Washington, D.C.: Sept. 9, 2003).

⁹GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, [GAO-06-982](#) (Washington, D.C.: Sept. 29, 2006). TWIC readers and related technologies operated outdoors in the harsh maritime environment can be affected by dirt, salt, wind, and rain.

¹⁰[GAO-10-43](#).

¹¹[GAO-11-657](#).

¹²Pub. L. No 109-347, § 104(a), 120 Stat. 1884, 1888 (codified at 46 U.S.C. § 70105(k)).

the technology, business processes, and operational impacts of deploying card readers at maritime facilities and vessels prior to issuing a final rule.¹³ Among other things, the SAFE Port Act required that DHS submit a report on the findings of the pilot program to Congress.¹⁴ DHS submitted its report to Congress on the findings of the TWIC reader pilot on February 27, 2012.¹⁵

The Coast Guard Authorization Act of 2010 required that the TWIC reader pilot report include, among other things, a comprehensive listing of the extent to which established metrics were achieved during the pilot program and that among other things, GAO conduct an assessment of the report's findings and recommendations.¹⁶ To meet this requirement, we addressed the following question:

- To what extent were the results from the TWIC reader pilot sufficiently complete, accurate, and reliable for informing Congress and the TWIC card reader rule?

To conduct our work, we assessed TWIC reader pilot test plans and results, as well as DHS's February 2012 report to Congress on the results of the TWIC reader pilot. We reviewed the extent to which pilot test plans were updated and used since we reported on them in November 2009.¹⁷ We also assessed the methods used to collect and analyze pilot data since the inception of the pilot in August 2008. We analyzed and compared the pilot data with the TWIC reader pilot report submitted to

¹³The SAFE Port Act required the Secretary to conduct a pilot program to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the maritime transportation system. 46 U.S.C. § 70105(k)(1)(A).

¹⁴46 U.S.C. § 70105(k)(4).

¹⁵Department of Homeland Security, *Transportation Worker Identification Credential Reader Pilot Program: In accordance with Section 104 of the Security and Accountability For Every Port Act of 2006, P.L. 109-347 (SAFE Port Act) Final Report*. Feb. 17, 2012.

¹⁶Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2989. Specifically, the report was to include (1) the findings of the pilot program with respect to key technical and operational aspects of implementing TWIC technologies in the maritime sector; (2) a comprehensive listing of the extent to which established metrics were achieved during the pilot program; and (3) an analysis of the viability of those technologies for use in the maritime environment, including any challenges to implementing those technologies and strategies for mitigating identified challenges.

¹⁷[GAO-10-43](#).

Congress to determine whether the findings in the report are based on sufficiently complete, accurate, and reliable data. In doing so, we reviewed TWIC reader pilot site reports from all of the sites and the underlying data to assess the extent to which data in these reports were consistent and complete. Additionally, we interviewed officials at DHS, TSA, and USCG with responsibilities for overseeing the TWIC program, as well as pilot officials responsible for coordinating pilot efforts with TSA and the independent test agent, about TWIC reader pilot testing approaches, results, and challenges. We compared the TWIC reader pilot effort with requirements in MTSA, the SAFE Port Act, and the Coast Guard Authorization Act of 2010. We further assessed the effort, including data collection and reporting, against established practices for designing evaluations and assessing the reliability of computer-processed data as well as internal control standards for collecting and maintaining records.¹⁸ Our investigators also conducted limited covert testing of TWIC program internal controls for acquiring and using TWIC cards at four maritime ports to update our understanding of the effectiveness of TWIC at enhancing maritime security since we reported on these issues in May 2011.¹⁹ The information we obtained from the four maritime ports is not generalizable across the maritime transportation industry as a whole, but provided additional perspectives and context on the TWIC program. Finally, we reviewed and assessed the security benefits presented in the TWIC reader notice of proposed rulemaking (NPRM) issued March 22, 2013, to determine whether the effectiveness of the noted security benefits were presented.²⁰ For additional details on our scope and methodology, see appendix I.

We conducted this performance audit from January 2012 to May 2013 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

¹⁸GAO, *Designing Evaluations: 2012 Revision*, [GAO-12-208G](#) (Washington, D.C.: Jan. 31, 2012); *Assessing the Reliability of Computer Processed Data*, [GAO-09-680G](#) (Washington, D.C.: July 1, 2009); and [GAO/AIMD-00-21.3.1](#), *Standards for Internal Control in the Federal Government* (Washington, D.C.: Nov. 1, 1999).

¹⁹See [GAO-11-657](#). The four ports tested as part of this limited covert testing update were selected because (1) we conducted covert testing at these locations during our prior review and (2) they are geographically dispersed across the United States, representing the East Coast, South, and Southwest.

²⁰78 Fed. Reg. 17,782 (Mar. 22, 2013).

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 objective. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

TWIC Program History and Our Prior Related Work

Following the terrorist attacks of September 11, 2001, the Aviation and Transportation Security Act (ATSA) was enacted in November 2001 and required TSA to work with airport operators to strengthen access controls to secure 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.²¹ In response, TSA established the TWIC program in December 2001.²² TWIC was originally envisioned as a nationwide transportation worker identity solution to be used by approximately 6 million credential holders across all modes of transportation, including seaports, airports, rail, pipeline, trucking, and mass transit facilities. In November 2002, MTSA further required DHS to issue a maritime worker identification card that uses biometrics to control access to secure areas of maritime transportation facilities and vessels.²³ TSA and USCG decided to implement TWIC initially in the maritime domain. Other transportation modes such as aviation have a preference for site-specific credentials.

As defined by DHS, and consistent with the requirements of MTSA, the purpose of the TWIC program is to design and field a common biometric credential for all transportation workers across the United States who require unescorted access to secure areas at MTSA-regulated maritime facilities and vessels. As stated in the TWIC mission needs statement, the TWIC program aims to meet the following mission needs:

²¹Pub. L. No. 107-71, § 106(c)(4), 115 Stat. 597, 610 (2001).

²²TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act of 2002 enacted on November 25, 2002. Pub. L. No. 107-296, 116 Stat. 2135.

²³46 U.S.C. § 70105.

-
- 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, and
 - 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.²⁴

In 2005, TSA conducted an analysis of alternatives and a cost-benefit analysis to identify possible options for addressing MTSA's requirement to develop a biometric transportation security card that would also meet the related mission needs specified above.²⁵ On the basis of these analyses, TSA determined that the best alternative was for the federal government to issue a single biometric credential that could be used across all vessels and maritime facilities, and for the government to manage all aspects of the credentialing process—enrollment, card issuance, and card revocation. TSA considered an alternative option based on a more decentralized and locally managed approach wherein MTSA-regulated facilities, vessels, and other port-related entities could issue their own credentials after individuals passed a TSA security threat assessment, but ultimately rejected the option (additional details are provided later in this report).

To help evaluate the TWIC program concept, TSA—through a private contractor—conducted prototype testing in 2004 and 2005 at 28 transportation facilities around the nation. However, in September 2006, we reported on the testing conducted by the contractor and identified challenges related to ensuring that the TWIC technology, such as biometric card readers, works effectively in the harsh maritime

²⁴Transportation Security Administration, *Mission Need Statement for the Transportation Worker Identification Credential (TWIC) Program*, Sept. 20, 2006.

²⁵Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Program Analysis of Alternatives Version 2.0*. Feb. 15, 2005, and *Transportation Worker Identification Credential (TWIC) Program Cost Benefit Analysis, Version 1.0*. Aug. 31, 2005.

environment.²⁶ We found that an independent assessment of the testing contractor's report identified problems with the report, such as inaccurate and missing information. As a result, the independent assessment recommended that TSA not rely on the contractor's final report on the TWIC prototype when making future decisions about the implementation of TWIC.

In 2006, the SAFE Port Act amended MTSA and directed the Secretary of Homeland Security to, among other things, implement a TWIC reader pilot to test the technology and operational impacts of deploying card readers at maritime facilities and vessels.²⁷ TSA initiated the pilot in August 2008.²⁸ This pilot was conducted with the voluntary participation of maritime port, facility, and vessel operators at 17 sites within the United States. In November 2009, we reported on the TWIC reader pilot design and planned approach, and found that DHS did not have a sound evaluation approach to ensure information collected through the TWIC reader pilot would be complete, accurate, and representative of deployment conditions.²⁹ Among other things, we recommended that an evaluation plan and data analysis plan be developed to guide the remainder of the pilot and to identify how DHS would compensate for areas where the TWIC reader pilot would not provide the information needed to report to Congress and implement the TWIC card reader rule. DHS concurred with this recommendation. The status of TSA's efforts to develop these plans is discussed later in this report. In addition, the Coast Guard Authorization Act of 2010 required that the findings of the pilot be included in a report to Congress, and that we assess the reported findings and recommendations.³⁰

²⁶[GAO-06-982](#).

²⁷Pub. L. No 109-347, § 104(a), 120 Stat. 1884, 1888 (codified at 46 U.S.C. § 70105(k)).

²⁸According to TSA, there were several factors that contributed to delays in commencing the pilot. These included (1) the voluntary nature of participation; (2) the first TWIC readers were not available for testing until July 2008, resulting in a 15-month delay in commencing the pilot; and (3) some facilities could acquire equipment or services quickly, while others required extensive bid processes or board of directors' approval.

²⁹[GAO-10-43](#).

³⁰Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2989.

In May 2011, we reported that internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limited the program's ability to provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals.³¹ We also reported that DHS had not assessed the TWIC program's effectiveness at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, we reported that DHS had not conducted a risk-informed cost-benefit analysis that considered existing security risks. We recommended, among other things, that DHS (1) assess TWIC program internal controls to identify needed corrective actions; (2) assess the TWIC program's effectiveness; and (3) use the information from the assessment 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 program objectives and mitigate existing security risks. DHS concurred with our recommendations and has taken steps to assess TWIC program internal controls. Appendix II summarizes key activities in the implementation of the TWIC program.

According to DHS documents, from fiscal year 2002 through fiscal year 2012, the TWIC program had funding and fee authority totaling \$393.4 million and the TWIC reader pilot cost approximately \$23 million.³² In issuing the credential rule, which required each maritime worker seeking unescorted access to secure areas of MTSA-regulated facilities and vessels to possess a TWIC, 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.³³ However, these figures did not include costs associated with implementing and operating card readers, as the credential rule did not require the installation or use of TWIC cards with readers. The notice of

³¹[GAO-11-657](#).

³²Over \$23 million had been made available to pilot participants from two Federal Emergency Management Agency (FEMA) grant programs—the Port Security Grant Program and the Transit Security Grant Program. Of the \$23 million, grant recipients agreed to spend nearly \$15 million on the TWIC reader pilot. However, DHS is unable to validate the exact amount grant recipients spent on the TWIC reader pilot, as rules for allocating what costs would be included as TWIC reader pilot costs versus other allowable grant expenditures were not defined. Sixteen of the 17 participating pilot sites were funded using these grants. In addition, TSA obligated an additional \$8.1 million of appropriated funds to support the pilot.

³³72 Fed. Reg. 3492, 3571 (Jan. 25, 2007).

proposed rulemaking published on March 22, 2013, estimated an additional cost of \$234.2 million (undiscounted) to implement readers at 570 facilities and vessels that the TWIC reader currently targets.³⁴ However, USCG does not rule out expanding reader requirements in the future. Appendix III contains additional program funding details.

TSA's Pilot to Test Key TWIC-Related Access Control Technologies

The TWIC reader pilot was intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. Accordingly, the pilot was to test the viability of using selected biometric card readers to read TWICs within the maritime environment. It was also to test the technical aspects of connecting TWIC readers to access control systems. The results of the pilot are to inform the development of a proposed rule requiring the use of electronic card readers with TWICs at MTSA-regulated vessels and facilities.³⁵

To conduct the TWIC reader pilot, TSA contracted with the Navy's Space and Naval Warfare Systems Command (SPAWAR) to serve as the independent test agent to plan, analyze, evaluate, and report on all test events. Furthermore, the Navy's Naval Air Systems Command (NAVAIR) conducted environmental testing of select TWIC readers.³⁶ In addition, TSA partnered with the maritime industry at 17 pilot sites distributed across seven geographic locations within the United States.³⁷ See

³⁴A notice of proposed rulemaking is published in the *Federal Register* and contains notices to the public of the proposed issuance of rules and regulations.

³⁵Based on the August 2008 pilot initiation date, the TWIC card reader rule was to be issued no later than 24 months from the initiation of the pilot, or by August 2010, and a report on the findings of the pilot was to be submitted 4 months prior, or by April 2010. 46 U.S.C. § 70105(k). However, TSA reported that there were challenges, such as pilot participation being voluntary, encountered during the pilot that resulted in delayed reporting.

³⁶SPAWAR is a component of the Department of the Navy. It develops and deploys advanced communications and information capabilities for the Navy and supports the full life cycle of product and services delivery, including initial research and development and acquisition services, among others. NAVAIR is housed in the Department of the Navy and provides support such as testing and evaluating systems operated by sailors and marines.

³⁷Pilot sites were located at the following locations: (1) Annapolis, Maryland; (2) Brownsville, Texas; (3) the Port Authority of New York / New Jersey and Staten Island, New York; (4) Long Beach and Los Angeles, California; (5) Norco, Louisiana; (6) Seattle, Washington; and (7) Vicksburg, Mississippi.

appendix IV for a complete listing of the pilot sites, locations, and types of maritime operation each represented. Levels of participation varied across the pilot sites. For example, at one facility, one pedestrian turnstile was tested out of 22 identified entry points. At another, the single vehicle gate was tested, but none of the seven pedestrian gates were tested. At a third facility with three pedestrian gates and 36 truck lanes, all three turnstiles and 2 truck lanes were tested. According to TSA, given the voluntary nature of the pilot, levels of participation varied across the pilot sites, and TSA could not dictate to the respective facilities and vessels specific and uniform requirements for testing.

The TWIC reader pilot, as initially planned, was to consist of three sequential assessments, with the results of each assessment intended to inform the subsequent ones. Table 1 highlights key aspects of the three assessments.

Table 1: Three Assessments Planned for the Transportation Worker Identification Credential (TWIC) Reader Pilot

Test name	Description
Initial technical test (ITT)	This assessment is laboratory based and designed to determine if selected biometric card readers meet TWIC card reader specifications, which include technical (including functional) and environmental requirements deemed necessary for use in the harsh maritime environment. ^a At the completion of initial technical testing, a test report was to be developed to prioritize all problems with readers based on their potential to adversely impact the maritime transportation facility or vessel. On the basis of this assessment, readers with problems that would severely impact maritime operations were not to be recommended for use in the next phase of testing.
Early operational assessment (EOA)	This assessment was to serve as an initial evaluation of the impact of TWIC reader implementation on the flow of commerce. Key results to be achieved as part of this assessment included obtaining essential data to inform development of the TWIC card reader rule, assessing reader suitability and effectiveness, and further refining reader specifications. As part of this assessment, maritime transportation facilities and vessels participating in the pilot were to select the readers they plan to test and install, and test readers as part of the test site's normal business and operational environment. The Transportation Security Administration's objective was to include pilot test participants that are representative of a variety of maritime transportation facilities and vessels in different geographic locations and environmental conditions.
System test and evaluation (ST&E)	Building on the results of the initial technical testing and the early operational assessment, the system test and evaluation was intended to evaluate the full impact of maritime transportation facility and vessel operators complying with a range of requirements anticipated to be included in the TWIC card reader rule. In addition, this evaluation was expected to establish a test protocol for evaluating readers prior to acquiring them for official TWIC implementation.

Source: GAO analysis of TSA documentation on the TWIC reader pilot.

^aTWIC card reader specifications were first published in September 2007 and updated on May 30, 2008.

To address time and cost constraints related to using the results of the TWIC reader pilot to inform the TWIC card reader rule, two key changes were made to the pilot tests in 2008. First, TSA and USCG inserted an initial reader evaluation as the first step of the initial technical test. This evaluation was an initial assessment of each reader's ability to read a TWIC.³⁸ Initiated in August 2008, the initial reader evaluation resulted in a list of biometric card readers from which pilot participants could select for use in the pilot rather than waiting for the entire ITT to be completed. Further, the list of readers that passed the initial reader evaluation was used by TSA and USCG to help select a limited number of readers for full functional and environmental testing.³⁹ Second, TSA did not require the TWIC reader pilot to be conducted in the sequence highlighted in table 1. Rather, pilot sites were allowed to conduct the early operational assessment and the system test and evaluation testing while ITT was under way.

Various reports were produced to document the results of each TWIC reader pilot assessment. An overall report was produced to document the ITT results conducted prior to testing at pilot sites. To document the results of testing at each of the 17 pilot sites, the independent test agent produced one EOA report and one ST&E report for each site. These reports summarized information collected from each of the pilot sites and trip reports documenting the independent test agent's observations during visits to pilot sites.

On February 27, 2012, DHS conveyed the results of the TWIC reader pilot by submitting the TWIC Reader Pilot Program report to Congress. On March 22, 2013, USCG issued a notice of proposed rulemaking that would, if finalized, require owners and operators of certain MTSAs-

³⁸The initial reader evaluation is officially known as the initial capability evaluation.

³⁹ITT full functional testing, or Functional Specification Conformance Test, was an evaluation of readers based on their ability to meet the TWIC specifications using 31 points of evaluation. As a result of this evaluation, the independent test agent was to provide a report to TSA on test metrics collected during functional testing to identify any functional or security problems related to reader performance. ITT full environmental testing, or Environmental Specification Conformance Test, included a series of tests to evaluate the card reader's ability to operate in the expected electrical and environmental conditions that exist in the coastal ports of the United States—such as humidity, salt, fog, and dust.

regulated vessels and facilities to use readers designed to work with TWICs.⁴⁰

TWIC Reader Pilot Results Are Not Sufficiently Complete, Accurate, and Reliable for Informing Congress and the TWIC Card Reader Rule

Challenges related to pilot planning, data collection, and reporting affect the completeness, accuracy, and reliability of the pilot test aimed at assessing the technology and operational impact of using TSA's TWIC with card readers. Moreover, according to our review of the pilot and TSA's past efforts to demonstrate the validity and security benefits of the TWIC program, the program's premise and effectiveness in enhancing security are not supported.

Shortfalls in Planning Affected the Completeness, Accuracy, and Reliability of Data Collected during the Pilot

As we previously reported, TSA encountered challenges in its efforts to plan the TWIC reader pilot. In November 2009, we reviewed and reported on the TWIC reader pilot design and planned approach for collecting data at pilot sites.⁴¹ For example, we reported that the pilot test and evaluation documentation did not identify how individual pilot site designs and resulting variances in the information collected from each pilot site were to be assessed. This had implications for both the technology aspect of the pilot as well as the business and operational aspect. We further reported that pilot site test designs may not be representative of future plans for using TWIC because pilot participants were not necessarily using the technologies and approaches they intend to use in the future when TWIC readers are implemented at their sites.⁴² As a result, we reported that there was a risk that the selected pilot sites and test methods would not result in the information needed to understand the impacts of TWIC nationwide. At the time, TSA officials told us that no specific unit of analysis, site selection criteria, or sampling methodology

⁴⁰78 Fed. Reg. 17,782 (Mar. 22, 2013).

⁴¹[GAO-10-43](#).

⁴²Officials at two of the seven pilot sites we visited at the time told us that the technology and processes expected to be in place during the pilot would likely not be the same as will be employed in the post-pilot environment, thereby reducing the reliability of the information collected at pilot locations.

was developed or documented prior to selecting the facilities and vessels to participate in the TWIC reader pilot.

As a result of these challenges, we recommended that DHS, through TSA and USCG, develop an evaluation plan to guide the remainder of the pilot that includes (1) performance standards for measuring the business and operational impacts of using TWIC with biometric card readers, (2) a clearly articulated evaluation methodology, and (3) a data analysis plan. We also recommended that TSA and USCG identify how they will compensate for areas where the TWIC reader pilot will not provide the necessary information needed to report to Congress and inform the TWIC card reader rule. DHS concurred with these recommendations.

While TSA developed a data analysis plan, TSA and USCG reported that they did not develop an evaluation plan with an evaluation methodology or performance standards, as we recommended. The data analysis plan was a positive step because it identified specific data elements to be captured from the pilot for comparison across pilot sites. If accurate data had been collected, adherence to the data analysis plan could have helped yield valid results. However, TSA and the independent test agent did not utilize the data analysis plan. According to officials from the independent test agent, they started to use the data analysis plan but stopped using the plan because they were experiencing difficulty in collecting the required data and TSA directed them to change the reporting approach. TSA officials stated that they directed the independent test agent to change its collection and reporting approach because of TSA's inability to require or control data collection to the extent required to execute the data analysis plan. However, TSA and USCG did not fully identify how they would compensate for areas where the pilot did not provide the necessary information needed to report to Congress and inform the TWIC card reader rule. For example, such areas could include (1) testing to determine the impact of the business and operational processes put in place by a facility to handle those persons that are unable to match their live fingerprint to the fingerprint template stored on the TWIC and (2) requiring operators using a physical access control system in conjunction with a TWIC to identify how they are protecting personal identify information and testing how this protection affects the speed of processing TWICs. While USCG commissioned two studies to help compensate for areas where the TWIC reader pilot will not

provide necessary information,⁴³ the studies did not compensate for all of the challenges we identified in our November 2009 report.⁴⁴ Such challenges included, for example, the impact of adding additional security protection on systems to prevent the disclosure of personal identity information and the related cost and processing implications.

In addition, our review of the TWIC reader pilot approach as implemented since 2009 and resulting pilot data identified some technology issues that affected the reliability of the TWIC reader pilot data. As DHS noted in its report to Congress, successful implementation of TWIC readers includes the development of an effective system architecture and physical access control system and properly functioning TWIC cards, among other things.⁴⁵ However, not all TWIC card readers used in the TWIC reader pilot underwent both environmental and functional tests in the laboratory prior to use at pilot sites as originally intended. Because of cost and time constraints, TSA officials instead conducted an initial evaluation of all readers included in the pilot to determine their ability to read a TWIC. These initial evaluations resulted in a list of 30 biometric TWIC card readers from which pilot participants could select a reader for use. However, of these 30 readers, 8 underwent functional testing and 5 underwent environmental testing. None of the TWIC card readers underwent and passed all tests.

TSA and independent test agent summary test results note that ambiguities within the TWIC card reader specification—the documented requirements for what and how TWIC card readers are to function—may have led to different interpretations and caused failures of tested TWIC systems. According to TSA, the readers that underwent laboratory-based

⁴³Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, a report prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011). Booz, Allen, Hamilton. *Port Facility Congestion Study, United States Coast Guard*, a report prepared for the United States Coast Guard, (McLean, Virginia: February 16, 2011).

⁴⁴[GAO-10-43](#).

⁴⁵For a TWIC-based access control system, system architecture refers to the selection, placement, and integration of systems required to make a decision about granting or denying access. Components of a TWIC-based access control system architecture may include, for example, the card readers, other systems or databases used (where needed) to make access control decisions, and the connectivity between the card readers and other systems or databases.

environmental and functional testing and were placed on the TSA list of acceptable readers did not have problems that would severely impact pilot site operations or prevent the collection of useful pilot data and therefore the readers were all available for use during the pilot. However, according to our review of the pilot documentation, TSA did not define what “severely impact” meant or performance thresholds for reader problems identified during laboratory-based environmental and functional testing that would severely impact pilot site operations or prevent the collection of useful pilot data. Further, according to TSA officials, TSA could not eliminate 1 of the readers that may have failed a test from the list of acceptable readers when other readers that had not been tested would be allowed on the list. According to TSA officials, doing so would have been an unfair disadvantage to the readers that were selected for the more rigorous laboratory-based environmental and functional testing. In addition, TSA did not provide pilot sites with the results of the laboratory-based environmental and functional testing. According to TSA, it signed confidentiality agreements with reader vendors, which prevented it from sharing this information. The results could have been used to help inform each pilot site’s selection of readers appropriate for its organization’s environmental and operational considerations. This may have hindered TSA’s efforts to determine if issues observed during the pilot were due to the TWIC, TWIC reader, or a facility’s access control system. Nonetheless, TSA determined that information collected during reader laboratory-based testing and at pilot sites was still useful for refining future TWIC reader specifications.

In addition, while TWIC cards are intended for use in the harsh maritime environment, the finalized TWIC cards did not undergo durability testing prior to testing at pilot sites. TSA selected card stock that had been tested in accordance with defined standards.⁴⁶ However, TSA did not conduct durability tests of the TWIC cards after they were personalized with

⁴⁶Card stock is a blank card that includes physical characteristics such as the antenna and computer chip. Card stock is used to manufacture TWIC cards. The card stock used by the TWIC program has been evaluated by the General Services Administration’s Federal Information Processing Standards (FIPS) 201 Evaluation Program to determine whether the card stock meets federal standards. These standards include various durability tests of blank card stock prior to approving the card stock for placement on the General Services Administration’s list of products approved for use by federal agencies.

security features, such as the TWIC holder's picture, or laminated.⁴⁷ According to TSA, technology reasons that may render a TWIC card damaged include, among others, breakage to the antenna or the antenna's connection to the card's computing chip.⁴⁸ Without testing the durability of personalized TWIC cards, the likelihood that TWIC cards and added security features can withstand the harsh maritime environment is unknown. According to TWIC program officials, each TWIC is tested to ensure it functions prior to being issued to an individual. However, the finalized TWIC card was not tested for durability to ensure that it could withstand the harsh maritime environment because doing so would be costly; TWIC is a fee-funded program, and the officials believed it would be unfair to pass on the cost to further test TWICs to consumers. However, testing TWIC credentials to ensure they can withstand the harsh maritime environment may prove to be more cost-effective, as it could minimize the time lost at access points and the TWIC holder's need to pay a \$60 replacement fee if the TWIC were to fail.

The importance of durability testing has been recognized by other government agencies and reported by GAO as a means to identify card failures before issuance. For example, the Department of Defense's (DOD) common access card—also used in harsh environments such as Afghanistan and other areas with severe weather conditions—has, according to DOD officials, been tested after personalization to ensure that it remains functional and durable.⁴⁹ DOD also assesses returned nonfunctioning common access cards to identify the potential cause of card failures. In addition, in June 2010, as part of our review of another

⁴⁷As we reported in April 2011, although not required to comply with FIPS-201, (Personal Identity Verification [PIV]) of Federal Employees and Contractors), as a policy decision, DHS and TSA decided to align the TWIC program with FIPS-201 standards where possible. To satisfy FIPS-201 security and technical interoperability requirements, a PIV card must be personalized and include identity information for the individual to whom the card is issued. Further, it must be free of defects such as fading and discoloration, not impede access to machine-readable information, and meet durability requirements. FIPS-201 requires durability tests to evaluate card material durability and performance. Card durability can be affected by what is added to the card upon completion of personalization. For example, adding laminated card finishes and security features may affect the durability of the finished card.

⁴⁸The antenna is the piece of technology needed for a contactless reader to communicate with a TWIC.

⁴⁹DOD's common access card is an identification card used by active-duty military personnel, DOD civilian employees, and eligible contractor personnel.

credential program, we recommended that the Department of State fully test or evaluate the security features on its Border Crossing Cards, including any significant changes made to the cards' physical construction, security features, or appearance during the development process.⁵⁰ Thus, durability testing TWIC cards after personalization could have reduced the pervasiveness of problems encountered with malfunctioning TWIC cards during the pilot.

As a result of the noted planning and preparation shortfalls, including (1) the absence of defined performance standards for measuring pilot performance, (2) variances in pilot site testing approaches without compensating measures to ensure complete and comparable data were collected, and (3) inadequate testing to ensure that piloted readers and TWICs worked as intended, the data TSA and the independent test agent collected on the technology and operational impacts of using TWIC at pilot sites were not complete, accurate, and reliable.

Data Collection Challenges Were Encountered during the TWIC Reader Pilot

In addition to the pilot planning challenges discussed above, we found that the data collected through the pilot are also not generalizable because of certain pilot implementation and data collection practices we identified.⁵¹ As required by the SAFE Port Act of 2006, the pilot was to

⁵⁰See GAO. *Border Security: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards*. [GAO-10-589](#) (Washington, D.C.: June 1, 2010). We reported that the Department of State (State) tested and evaluated the security of prototypes of the passport card, which did not include key features such as the background artwork, personalization features, and other security features that were added or changed for the final passport card. We recommended that State fully test or evaluate the security features on the cards as they will be issued, including any significant changes made to the cards' physical construction, security features, or appearance during the development process. State concurred and reported taking actions to address the recommendation.

⁵¹Collected operational and performance data cannot be generalized across each pilot site or nationally across all pilot sites where use of TWIC will be required because neither the pilot sites nor access points tested were selected randomly. According to USCG officials, USCG believes that cost data derived from the pilot can be extrapolated. However, on the basis of our analysis and review of pilot data, given the limitations of collected cost data, including that pilot sites did not necessarily implement readers and associated access control systems as they intend in the future, use of cost data derived from the pilot should be limited and used with caution, if at all. Reliable data on the pervasiveness of TWIC card issues, access control systems erroneously preventing access to facilities, queues at access points, and ongoing reader and related access control system operations and maintenance costs, among others, are needed to reliably determine the economic cost impact of using TWIC with readers.

test the technology and operational impacts of deploying transportation security card readers at secure areas of the marine transportation system. In addition, as set forth in the TWIC test and evaluation master plan, the TWIC reader pilot was to provide accurate and timely information necessary to evaluate the economic impact of a nationwide deployment of TWIC card readers at over 16,400 MTSA-regulated facilities and vessels, and was to be focused on assessing the use of TWIC readers in contactless mode.⁵² However, data were collected and recorded in an incomplete and inconsistent manner during the pilot, further undermining the completeness, accuracy, and reliability of the data collected at pilot sites. Table 2 presents a summary of TWIC reader pilot data collection and supporting documentation reporting weaknesses that we identified that affected the completeness, accuracy, and reliability of the pilot data, which we discuss in further detail below.

Table 2: Weaknesses in the Transportation Worker Identification Credential (TWIC) Reader Pilot Affecting the Completeness, Accuracy, and Reliability of Data Collected

1. Installed TWIC readers and access control systems could not collect required data on TWIC reader use, and TSA and the independent test agent did not employ effective compensating data collection measures.
2. Reported transaction data did not match underlying documentation.
3. Pilot documentation did not contain complete TWIC reader and access control system characteristics.
4. Transportation Security Administration (TSA) and the independent test agent did not record clear baseline data for comparing operational performance at access points with TWIC readers.
5. TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.
6. Pilot participants did not document instances of denied access.
7. TSA and the independent test agent did not collect consistent data on the operational impact of using TWIC cards with readers.
8. Pilot site reports did not contain complete information about installed TWIC readers' and access control systems' design.

Source: GAO.

⁵²U.S. Department of Homeland Security, Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Contactless Biometric Card and Reader Capability Pilot Test, Test and Evaluation Master Plan (TEMP)*, approved December 2007. As used in this report, contactless mode refers to the use of TWIC readers for reading TWIC cards without requiring that a TWIC card be inserted into or make physical contact with a TWIC reader.

1. Installed TWIC readers and access control systems could not collect required data on TWIC reader use, and TSA and the independent test agent did not employ effective compensating data collection measures. The TWIC reader pilot test and evaluation master plan recognizes that in some cases, readers or related access control systems at pilot sites may not collect the required test data, potentially requiring additional resources, such as on-site personnel, to monitor and log TWIC card reader use issues. Moreover, such instances were to be addressed as part of the test planning. However, the independent test agent reported challenges in sufficiently documenting reader and system errors. For example, in its monthly communications with TSA, the independent test agent reported that the logs from the TWIC readers and related access control systems were not detailed enough to determine the reason for errors, such as biometric match failure, an expired TWIC card, or that the TWIC was identified as being on the list of revoked credentials. The independent test agent further reported that the inability to determine the reason for errors limited its ability to understand why readers were failing, and thus it was unable to determine whether errors encountered were due to TWIC cards, readers, or users, or some combination thereof. As a result, according to the independent test agent, in some cases the TWIC readers and automated access control systems at various pilot sites were not capable of collecting the data required to assess pilot results. According to the independent test agent, this was primarily due to the lack of reader messaging standards—that is, a set of standard messages readers would display in response to each transaction type. Some readers used were newly developed by vendors, and some standards were not defined, causing inconsistencies in the log capabilities of some readers.⁵³ The independent test agent noted that reader manufacturers and system integrators—or individuals or companies that integrate TWIC-related systems—were not all willing to alter their systems' audit logs to collect the required information, such as how long a transaction might take prior to granting access. Both TSA and the independent test agent agree that this issue limited their ability to collect the data needed for assessing pilot results.

According to TSA officials, TSA allowed pilot participants to select their own readers and related access control systems and audit logs.

⁵³The independent test agent could not provide an exact count of the readers with log capability inconsistencies.

Consequently, TSA could not require that logs capable of meeting pilot data collection needs be used. In addition, TSA officials noted that determining the reason for certain errors, such as biometric match failures, could be made only while the independent test agent was present and had the time and ability to investigate the reason that a TWIC card had been rejected by a reader for access. On average, the independent test agent visited each pilot participant seven times during the early operational assessment and system test and evaluation testing period. TSA further noted that the development or use of alternative automated data collection methods would have been costly and would have required integration with the pilot site's system. However, given that TSA was aware of the data needed from the pilot sites prior to initiating testing and the importance of collecting accurate and consistent data from the pilot, proceeding with the pilot without implementing adequate compensating mechanisms for collecting requisite data or adjusting the pilot design accordingly is inconsistent with the basic components of effective evaluation design and renders the results less reliable.

2. Reported transaction data did not match underlying documentation. A total of 34 pilot site reports were issued by the independent test agent.⁵⁴ According to TSA, the pilot site reports were used as the basis for DHS's report to Congress. We separately requested copies of the 34 pilot site reports from both TSA and the independent test agent. In comparing the reports provided, we found that 31 of the 34 pilot site reports provided to us by TSA did not contain the same information as those provided by the independent test agent.⁵⁵ Differences for 27 of the 31 pilot site reports pertained to how pilot site data were characterized, such as the baseline throughput time used to compare against throughput times observed during two phases of testing: early operational assessment and systems test and evaluation. For example, TSA inserted USCG's 6-second visual inspection estimate as the baseline throughput time measure for all pilot site access points in its amended pilot site reports instead of the actual throughput time collected and reported by the independent test agent during baseline data

⁵⁴The independent test agent was to conduct two phases of testing—EOA and ST&E—at the 17 pilot sites. The independent test agent issued 2 pilot site reports for each of the 17 pilot sites—1 based on EOA tests and the other based on ST&E tests—for a total of 34 pilot site reports.

⁵⁵In total, we reviewed 68 reports; 34 provided by TSA and 34 provided by the independent test agent.

collection efforts.⁵⁶ However, at two pilot sites, Brownsville and Staten Island Ferry, transaction data reported by the independent test agent did not match the data included in TSA's reports. For example, of the 15 transaction data sets in the Staten Island Ferry ST&E report, 10 of these 15 data sets showed different data reported by TSA and the independent test agent. These differences were found in the weekly transactions and the sum total of valid and invalid transactions.⁵⁷

According to TSA officials, it used an iterative process to review and analyze pilot data as the data became available to it from the pilot participant sites. In addition, TSA officials noted that the independent test agent's reports were modified in order to "provide additional context" and consistent data descriptions, and to present data in a more usable or understandable manner. Specifically, according to TSA officials, they and USCG officials believed that they had more knowledge of the data than the independent test agent and there was a need, in some cases, for intervening and changing the test reports in order to better explain the data. USCG officials further noted that the independent test agent's draft reports were incomplete and lacked clarity, making revisions necessary to make the information more thorough. TSA also reported that it inadvertently used an earlier version of the report and not the final September 2011 site reports provided by the independent test agent to prepare the report to Congress.

In addition to differences found in the EOA and ST&E pilot site reports, we found differences between the data recorded during the independent test agent's visits to pilot sites versus data reported in the EOA and ST&E

⁵⁶According to TSA, it applied the 6-second baseline for visually inspecting a TWIC to account for the artificially short measured inspection times at some facilities where security personnel were observed allowing access without completing the three-step visual verification process required by USCG regulations: (1) checking the card expiration date, (2) comparing the photo on the card against the worker presenting the card, and (3) examining one of the security features on the card. USCG and TSA concurred that a minimum of 6 seconds is required to complete a compliant visual inspection. In addition, the 6-second baseline was also inserted at sites where the recorded baseline was longer than 6 seconds.

⁵⁷In addition to discrepancies observed in recorded transaction data for the Brownsville and Staten Island Ferry pilot sites, TSA did not collect transaction data at two pilot sites during the ST&E phase or throughput data at three pilot sites. The ST&E phase was intended to evaluate the full impact of facility and vessel operators complying with a range of anticipated identity verification requirements to be established through the TWIC reader rule.

pilot site reports. Data recorded during the independent test agent's visits to pilot sites in trip reports were to inform final pilot site reports. The independent test agent produced 76 trip reports containing throughput data. We examined 34 of the 76 trip reports and found that all 34 trip reports contained data that were excluded or did not match data reported in the EOA and ST&E pilot site reports completed by the independent test agent. According to the independent test agent, the trip reports did not match the EOA and ST&E pilot site reports because the trip reports contained raw data that were analyzed and prepared for presentation in the participant EOA and ST&E pilot site reports. However, this does not explain why data reported by date in trip reports do not match related data in the EOA and ST&E pilot site reports. Having inconsistent versions of final pilot site reports, conflicting data in the reports, and data excluded from final reports without explanation calls into question the accuracy and reliability of the data.

3. Pilot documentation did not contain complete TWIC reader and access control system characteristics. Pilot documentation did not always identify which TWIC readers or which interface (e.g., contact or contactless interface) the reader used to communicate with the TWIC card during data collection. For example, at one pilot site, two different readers were tested. However, the pilot site report did not identify which data were collected using which reader. Likewise, at pilot sites that had readers with both a contact and a contactless interface, the pilot site report did not always identify which interface was used during data collection efforts. According to TSA officials, sites were allowed to determine which interface to use based on their business and operational needs. According to the independent test agent, it had no control over what interface pilot sites used during testing if more than one option was available. Consequently, pilot sites could have used the contactless interface for some transactions and the contact interface for others without recording changes. The independent test agent therefore could not document with certainty which interface was used during data collection efforts. Without accurate documentation of information such as this, an assessment of TWIC reader performance based on interface cannot be determined. This is a significant data reliability issue, as performance may vary depending on which interface is used, and in accordance with the TWIC reader pilot's test and evaluation master plan, use of the contactless interface was a key element to be evaluated during the pilot.

4. TSA and the independent test agent did not record clear baseline data for comparing operational performance at access points with

TWIC readers. Baseline data, which were to be collected prior to piloting the use of TWIC with readers, were to be a measure of throughput time, that is, the time required to inspect a TWIC card and complete access-related processes prior to granting entry. This was to provide the basis for quantifying and assessing any TWIC card reader impacts on the existing systems at pilot sites.⁵⁸ Pilot documentation shows that baseline throughput data were collected for all pilot sites. However, it is unclear from the documentation whether acquired data were sufficient to reliably identify throughput times at truck, other vehicle, and pedestrian access points, which may vary. It is further unclear whether the summary baseline throughput data presented are based on a single access point, an average from all like access points, or whether the data are from the access points that were actually tested during later phases of the pilot. Further complicating the analysis of baseline data is that there was a TSA version of the baseline report and a separate version produced by the independent test agent, and facts and figures in each do not fully match. Where both documents present summary baseline throughput data for each pilot site, the summary baseline throughput data differ for each pilot site. For example, summary baseline throughput data at one pilot site is reported as 4 minutes and 10 seconds in one version of the report but is reported as 47 seconds in the other report. As a result, the accuracy and reliability of the available baseline data are questionable. Further, according to TSA, where summary throughput data were not included in the baseline report, the independent test agent's later site reports did contain the data.

5. TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards. TSA officials observed malfunctioning TWICs during the pilot, largely because of broken antennas. The antenna is the piece of technology needed for a contactless reader to communicate with a TWIC. If a TWIC with a broken antenna was presented for a contactless read, the reader would not identify that a TWIC had been presented, as the broken antenna would not communicate TWIC information to a contactless reader. In such instances, the reader would not log that an access attempt had been made and failed. Individuals holding TWICs with bad antennas had presented their TWICs at contactless readers; however, the readers did

⁵⁸Baseline data were to include, among other things, throughput times, the number and type of access points at a pilot site, the transactions (traffic) through each access point, and the populations accessing these points prior to TWIC reader installation.

not document and report each instance that a malfunctioning TWIC was presented. Instead, as noted by pilot participants and confirmed by TSA officials, pilot sites generally conducted visual inspections when confronting a malfunctioning TWIC and granted the TWIC holder access. While in some cases the independent test agent used a card analysis tool to assess malfunctioning TWICs, TSA officials reported that neither they nor the independent test agent documented the overall number of TWICs with broken antennas or other damage. According to TSA officials, the number of TWICs with broken antennas or other damage was not tracked because failed TWIC cards could be tracked only if an evaluator was present, had access to a card analysis tool, and had the cooperation of the pilot participants to hold up a worker's access long enough to confirm that the problem was the TWIC card and not some other factor. However, it is unclear why TSA was unable to provide a count of TWICs with broken antennas or other damage based on the TWIC cards that were analyzed with the card analysis tool.

While TSA could not provide an accounting of TWICs with broken antennas or other damage experienced during the pilot, pilot participants and other data collected provide additional context and perspective for understanding the nature and extent of TWIC card failure rates during the pilot. Officials at one pilot container facility told us that a 10 percent failure rate would be unacceptable and would slow down cargo operations. However, according to officials from two pilot sites, approximately 70 percent of the TWICs they encountered when testing TWICs against contactless readers had broken antennas or malfunctioned. Further, a separate 2011 report commissioned and led by USCG identified problems with reading TWICs in contactless mode during data collection.⁵⁹ This report identified one site where 49 percent of TWICs could not be read in contactless (or proximity⁶⁰) mode, and two other sites where 11 percent and 13 percent of TWICs could not be read in contactless mode. Because TWIC cards malfunctioned, they could not be detected by readers. Accordingly, individuals may have made multiple attempts to get the TWIC reader to read the TWIC card; however, each attempt was not

⁵⁹Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011).

⁶⁰As used in this report, reading a card in proximity mode is the same as reading a card in contactless mode.

recorded and thus TSA does not have an accurate accounting of the number of attempts or time it may have taken to resolve resulting access issues. Consequently, assessments of the operational impacts of using TWIC with readers using the collected data alone should be interpreted cautiously as they may be based on inaccurate data.

In discussing these failure rates with TSA officials, the officials reported that TSA does not have a record of a pilot participant reporting a 70 percent failure rate.⁶¹ In addition, they believe that the failure rates reported by pilot sites and the separate USCG-commissioned report are imperfect because they did not have the card analysis tool necessary to confirm a failed TWIC card, and instances where a failed TWIC card was presented at a pilot site could be documented only when the independent test agent was present at the site with a card analysis tool. However, a contractor from TSA visited the facility where the USCG report notes that 49 percent of TWICs could not be read in contactless mode and found that 60 out of 110 of TWIC cards checked, or 54.5 percent, would not work in contactless mode. TSA officials agreed that TWIC card failure rates were higher than anticipated and stated that TSA is continuing to assess TWIC card failures to identify the root cause of the failures and correct for them. TSA is also looking to test the TWIC cards at facilities that have not previously used TWIC readers to get a better sense of how inoperable TWIC cards might affect a facility operationally.

6. Pilot participants did not document instances of denied access.

Incomplete data resulted from challenges documenting how to manage individuals with a denied TWIC across pilot sites. The independent test agent reported that facility security personnel were unclear on how to process people who are denied access by a TWIC reader because of a biometric mismatch or other TWIC card issue. In these cases, pilot site officials would need to receive input from USCG as to whether to grant or deny access to an individual presenting a TWIC card that had been denied. According to TSA officials, during the pilot, if a TWIC reader denied access to a TWIC, the facility could visually inspect the TWIC, as allowed under current regulation, and grant the individual access. However, TSA and the independent test agent did not require pilot participants to document when individuals were granted access based on

⁶¹According to TSA officials, workers were not required to replace malfunctioning cards during the pilot. Therefore, a worker could present the same malfunctioning card to a reader upon each entry to a facility.

a visual inspection of the TWIC, or deny the individual access as may be required under future regulation. This is contrary to the TWIC reader pilot test and evaluation master plan, which calls for documenting the number of entrants “rejected” with the TWIC card reader system operational as part of assessing the economic impact. Without such documentation, the pilot sites were not completely measuring the operational impact of using TWIC with readers.

7. TSA and the independent test agent did not collect consistent data on the operational impact of using TWIC cards with readers.

TWIC reader pilot testing scenarios included having each individual present his or her TWIC for verification; however, it is unclear whether this actually occurred in practice. For example, at one pilot site, the independent test agent did not require each individual to have his or her TWIC checked during throughput data collection.⁶² Officials at the pilot site noted that during testing, approximately 1 in 10 individuals was required to have his or her TWIC checked while entering the facility because of concerns about causing a traffic backup. They said that this approach was used because pilot site officials believed that reading each TWIC would have caused significant congestion. However, the report for the pilot site does not note this selective use of the TWIC card. In addition, officials from another pilot site reported that truck drivers could elect to go to other lanes that were not being monitored during throughput time collection. Officials at this pilot site noted that truck drivers, observing congestion in lanes where throughput time was being collected, used other lanes to avoid delays. This was especially the case when the tested truck lane was blocked to troubleshoot TWIC card and reader problems. However, the pilot site report did not record congestion issues or the avoidance of congestion issues by allowing truck drivers to use alternative lanes where TWIC readers were not being tested. TSA officials also noted that another pilot site would allow trucks entry without using a TWIC reader on an ad hoc basis during the pilot to prevent congestion, making it difficult to consistently acquire the data needed to

⁶²Throughput data include the timing of the approach, credential check and clearance (if applicable), and physical movement through the point of entry. For the TWIC reader pilot, throughput data collection for truck and vehicle traffic was to begin once the truck or vehicle came to a complete stop at the access point and end once the truck or vehicle pulled away from the access point. The timing of pedestrian throughput may be calculated from the time an individual presents his or her TWIC or when the person comes within 2 feet of the access point (depending on the access process) and end once the access point is ready to receive the next entrant.

accurately assess the operational impacts, such as the truck congestion resulting from TWIC cards with readers. Despite the noted deviations in test protocols, the reports for these pilot sites do not note that these deviations occurred.

In commenting on this issue, TSA officials noted that these deviations occurred most frequently at those facilities with multiple truck or pedestrian access points where readers were installed at a few access points. Most commonly these facilities were large container terminals. Because of the voluntary nature of the pilot, TSA elected to primarily use reader performance data from facilities that did not install and use readers at all access points. TSA officials further noted that the impact of readers on operations at these facilities necessarily was discounted in the final report to Congress. However, pilot documentation shows that container terminals held the largest population of individuals potentially requiring the use of a TWIC. Noting deviations such as those described above in each pilot site report would have provided important perspective by identifying the limitations of the data collected at the pilot site and providing context when comparing the pilot site data with data from other pilot sites. Further, identifying the presence of such deviations could have helped the independent test agent and TSA recognize the limitations of the data when using them to develop and support conclusions for the pilot report on the business and operational impact of using TWICs with readers.

8. Pilot site reports did not contain complete information about installed TWIC readers' and access control systems' design. TSA and the independent test agent tested the TWIC readers at each pilot site to ensure they worked before individuals began presenting their TWIC cards to the readers during the pilot. As part of this test, information on how each TWIC reader communicated with TWICs and related access control systems was to be documented. In accordance with TWIC test plans, this testing was to specify, among other things, whether the TWIC reader (1) was contactless or required contact with a TWIC, (2) communicated with a facility's physical access control system(s) through a wired or wireless conduit, or (3) granted or denied access to a TWIC holder itself or relied on a centralized access system to make that determination. However, the data gathered during the testing were incomplete. For example, 10 of 15 sites tested readers for which no

record of system design characteristics were recorded.⁶³ In addition, pilot reader information was identified for 4 pilot sites but did not identify the specific readers or associated software tested. Further, 1 pilot site report included reader information for another pilot site and none for its own. This limited TSA's ability to assess performance results by various reader and access control system characteristics. The absence of this information is particularly important, as it was the only source of data recorded at pilot sites where reader and operational throughput performance could be assessed at a level of granularity that would allow for the consideration of the array of reader, system design, and entry process characteristics. According to TSA officials, collecting these data was the independent test agent's responsibility, but the independent test agent did not record and provide all required data. The independent test agent maintains that the data are present. However, we reviewed the documentation, and we did not find the data.

As we have previously reported, the basic components of an evaluation design include identifying information sources and measures, data collection methods, and an assessment of study limitations, among other things.⁶⁴ We further reported that care should be taken to ensure that collected data are sufficient and appropriate,⁶⁵ and that measures are incorporated into data collection to ensure that data are accurate and reliable.⁶⁶ Data may not be sufficiently reliable if (1) significant errors or incompleteness exists in some of or all the key data elements,⁶⁷ and (2) using the data would probably lead to an incorrect or unintentional message.⁶⁸ Moreover, in accordance with *Standards for Internal Control*

⁶³The reported figures exclude Brownsville and Staten Island Ferry pilot sites because of the extent of reporting deficiencies identified in reported data for these sites.

⁶⁴[GAO-12-208G](#).

⁶⁵Sufficiency refers to the quantity of evidence. Appropriateness refers to the relevance, validity, and reliability of the evidence in supporting the evaluation objectives.

⁶⁶Accuracy refers to the extent that recorded data reflect the actual underlying information. Consistency, a subcategory of accuracy, refers to the need to obtain and use data that are clear and well defined enough to yield similar results in similar analyses. For example, if data are entered at multiple sites, inconsistent interpretation of data entry rules can lead to data that, taken as a whole, are unreliable.

⁶⁷Completeness refers to the extent that relevant records are present and the fields in each record are populated appropriately.

⁶⁸[GAO-09-680G](#).

in the Federal Government, controls are to be designed to help ensure the accurate and timely recording of transactions and events. Properly implemented control activities help to ensure that all transactions are completely and accurately recorded.⁶⁹ Having measures in place to ensure collected data are complete, are not subject to inappropriate alteration, and are collected in a consistent manner helps ensure that data are accurate and reliable. However, as discussed in the examples above, TSA and the independent test agent did not take the steps needed to ensure the completeness, accuracy, and reliability of TWIC reader data collected at pilot sites, and the pilot lacked effective mechanisms for ensuring that transactions were completely and consistently recorded.

According to TSA, a variety of challenges prevented TSA and the independent test agent from collecting pilot data in a complete and consistent fashion. Among the challenges noted by TSA, (1) pilot participation was voluntary, which allowed pilot sites to stop participation at any time or not adhere to established testing and data collection protocols; (2) the independent test agent did not correctly and completely collect and record pilot data; (3) systems in place during the pilot did not record all required data, including information on failed TWIC card reads and the reasons for the failure; and (4) prior to pilot testing, officials did not expect to confront problems with nonfunctioning TWIC cards. Additionally, TSA noted that it lacked the authority to compel pilot sites to collect data in a way that would have been in compliance with federal standards. In addition to these challenges, the independent test agent identified the lack of a database to track and analyze all pilot data in a consistent manner as an additional challenge to data collection and reporting. The independent test agent, however, noted that all data collection plans and resulting data representation were ultimately approved by TSA and USCG. However, our review of pilot test results shows that because the resulting pilot data are incomplete, inaccurate, and unreliable, they should not be used to help inform the card reader rule. While TSA's stated challenges may have hindered TWIC reader pilot efforts, planning and management shortfalls also resulted in TWIC reader pilot data being incomplete, inaccurate, and unreliable. The challenges TSA and the independent test agent confronted during the pilot limited their data collection efforts, which were a critical piece of the assessment

⁶⁹[GAO/AIMD-00-21.3.1.](#)

of the technology and operational impacts of using TWIC at pilot sites that were to be representative of actual deployment conditions.

Issues with DHS's Congressional Report on the Pilot and the Validity of the TWIC Security Premise Raise Concerns about the Effectiveness of the TWIC Program

DHS's Report to Congress Presented Findings and Lessons Learned That Were Not Always Supported by the Collected Data

As required by the SAFE Port Act and the Coast Guard Authorization Act of 2010, DHS's report to Congress on the TWIC reader pilot presented several findings with respect to technical and operational aspects of implementing TWIC technologies in the maritime environment. DHS reported the following, among other findings:

1. Despite facing a number of challenges, the TWIC reader pilot obtained sufficient data to evaluate reader performance and assess the impact of using readers at ports and maritime facilities.
2. A biometric match may take longer than a visual inspection alone but not long enough to cause access point throughput delays that would negatively impact business operations.
3. When designed, installed, and operated in manners consistent with the business considerations of the facility or vessel operation, TWIC readers provide an additional layer of security by reducing the risk that an unauthorized individual could gain access to a secure area.

In addition, the report noted a number of lessons learned. For example, TWIC cards were found to be sensitive to wet conditions, and users experienced difficulty reading messages on the screens of readers not shielded from direct sunlight, which prevented users from determining the cause of access denial, among other things. According to officials from TSA and DHS's Screening Coordination Office, many of these lessons learned did not require a pilot in order to be identified, but the pilot did make a positive contribution by helping to validate these lessons learned. Additionally, officials from DHS's Screening Coordination Office noted that they believe that the report to Congress included a comprehensive

listing of the extent to which established metrics were achieved during the pilot program, as required by the Coast Guard Authorization Act of 2010.

However, according to our review, the findings and lessons learned in DHS's report to Congress were based on incomplete or unreliable data, and thus should not be used to inform the development of the future regulation on the use of TWIC with readers. Specifically, incomplete TWIC cost data and unreliable access point throughput time data result in an inaccurate description of the impact of TWIC on MTSA-regulated facilities and vessels. Further, data on the security benefits of TWIC were not collected as part of the pilot and therefore the statements made in DHS's report to Congress are not supported by the pilot data.

Reported Costs

DHS's report identified costs for implementing TWIC readers during the pilot. However, the costs reported by DHS do not represent the full costs of operating and maintaining TWIC readers and related systems within a particular site, or the cost of fully implementing TWIC at all sites. First, DHS's reported costs for implementing TWIC with readers during the pilot did not consistently reflect the costs of implementing TWIC at all access points needed for each facility. For example, DHS's report correctly notes that 2 container facilities did not implement TWIC readers at all access points and are therefore not reflective of full implementation. However, on the basis of our analysis and interviews with pilot site officials, at least 5 of the remaining pilot sites would need to make additional investments in readers, totaling 7 pilot sites requiring investments beyond reported expenditures. For example, officials at 2 pilot sites told us that they would need to invest in and install additional readers if reader use was required by regulation. Officials at 3 pilot sites told us that their investment in TWIC readers during pilot testing was not representative of how they would invest in TWIC if regulation required that an individual's TWIC be checked with a reader at each entry.⁷⁰ Second, we found that reported implementation costs did not match TSA's supporting documentation for 4

⁷⁰Specifically, 2 of 3 pilot sites tested portable readers alone, which required a limited investment, but would install fixed readers if readers were required by regulation to better address their needs. The security official from the third pilot site that primarily tested stand-alone fixed readers told us that his preference, if reader use is required, would be to use networked readers connected to a centralized access control system for making access determinations.

of 17 pilot sites. TSA told us that this discrepancy may be due to having multiple versions of cost data available and relying on different cost documents when compiling the cost data in the DHS report to Congress.⁷¹ The lack of complete and accurate cost data limits the usefulness of the information provided to Congress and does not help inform the development of the future regulation on the use of TWIC with readers.

In addition, DHS reported that facilities and vessels that cease issuing site-specific badges and instead use the TWIC card as the only identification needed for access may benefit financially by reducing card management operational costs associated with identity vetting, card inventory, printing equipment, and issuance infrastructure. However, according to TSA, data in support of this finding are based on the statement of one pilot participant who anticipated utilizing the TWIC and not issuing facility badges for access control. Further, DHS's Screening Coordination Office officials noted that the proximity and bar code cards that facilities currently use do not contain the same level of security features that the TWIC card does. However, a related March 2011 study on the use of TWIC with readers commissioned and led by USCG noted that there are significant reliability problems with using TWIC cards, which cost \$60 each to replace, in the contactless mode.⁷² The report further notes that off-the-shelf industry standard proximity and bar code cards are already inexpensively produced and managed at various facilities; are considered much more functionally reliable than the TWIC; and provide better overall security, since the cards and associated access control systems—such as readers and centralized databases—are less prone to failure.

Access Point Throughput Time versus Reader Response Time

DHS reported that observing differences in throughput times (i.e., entry times) at access points would be most relevant to determining the impact

⁷¹According to our analysis, the differences in reported implementation costs varied, with the largest being approximately \$286,500.

⁷²Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*: Prepared for the U.S. Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011).

of readers on business operations.⁷³ However, the times and comparisons presented in DHS's report were not throughput times gathered at pilot sites, but reader response times gathered during laboratory testing. The differences between throughput time and reader response times can vary significantly. For example, as recorded during the pilot, throughput time at a facility using a TWIC card reader was 1 minute and 36 seconds, whereas reader response time at the facility was 11 seconds. As noted by DHS, throughput time accounts for conditions at a particular facility or access point, including individual processes. In addition, measuring throughput time with TWIC readers and related systems can also capture variances due to system connectivity (e.g., hardwired or wireless connections), installed readers and interfaces, weather, and integration with access control or other business-related systems—all representative of real-world experiences at a given location or type of access point.

In contrast, reader response time, as reported by DHS, measures the amount of time a TWIC reader takes to determine whether a TWIC is valid in controlled laboratory settings. Measuring reader response time alone is valuable, as it can help a site determine what amount of increase or decrease in throughput time may be due to TWIC systems alone rather than business processes. However, DHS's reporting of reader response time data was not based on a specific pilot site or group of sites. Instead, it was based on lab testing, which is not representative of the technology challenges sites may face in practice, such as time lags due to the distance between a reader and supporting computing system, types of infrastructure available to implement the TWIC system, or the various variables that could delay actual transaction times. Accordingly, DHS's reporting of reader response time is not an effective measure of response time in a real-world environment and therefore is not an accurate representation of response times that might be experienced at maritime ports and facilities.

⁷³DHS's report to Congress stated the following: "Although reader response time [transaction time] data was acquired during the pilot, throughput time data was most relevant to determining the impact of readers on business operations. Throughput time measured the time it took to clear an access point using readers instead of conducting a visual inspection of the TWIC card. Activities beyond verifying the TWIC card and identity often occur at access points. Additionally, turnstile or gate opening times vary among access points. By using throughput times, these differences were accounted for, leaving only the variance of visual inspection versus reader times for comparison."

Reported Enhanced Security Findings Have Not Been Validated

DHS's report to Congress stated that "when designed, installed, and operated in manners consistent with the business considerations of the facility or vessel operations, TWIC readers provide an additional layer of security by reducing the risk that an unauthorized individual could gain access to a secure area." Further, in a written statement by DHS officials presented before Congress on June 28, 2012, DHS officials stated that TWIC enhances port facility and vessel security and that the pilot operation also highlighted security and operational benefits associated with readers, including the automation of access control, so that regular users could use their TWICs for quick and easy processing into a port.⁷⁴ However, USCG told us that assessment of security benefits was outside the scope of the TWIC reader pilot. Further, TSA confirmed that data regarding the security enhancements provided by TWIC were not collected during the pilot because that was neither the goal nor the legislative mandate of the TWIC reader pilot. Such data might include, for example, data on the number of people turned away at pilot access points for security infractions, information from covert testing at pilot sites, or other types of data to show enhanced security resulting from the implementation of TWIC.

Further, a March 2011 study commissioned by USCG to provide additional data needed for the regulatory analysis for the TWIC card reader rule concluded that "the current TWIC card and readers do not provide the seamless functionality, or security, as originally envisioned."⁷⁵ The study identified that the large numbers of TWIC card failures and inability of facilities to determine why a TWIC card is not working, or speedily determine why an employee's TWIC is on TSA's list of canceled cards, cause facilities to ignore the canceled card list and overlook broken or nonfunctional TWIC cards. The study noted that these shortfalls may significantly decrease facility security, especially when compared with a facility-controlled system where the facility issues its own credentials and uses established technologies. The study concluded that an increase in

⁷⁴U.S. Department of Homeland Security, Joint Written Statement of Kelli Ann Walther, Acting Deputy Assistant Secretary, Screening Coordination Office, Office of Policy, and Rear Admiral Joseph Servidio, Assistant Commandant for Prevention Policy, U.S. Coast Guard, Before the House Committee on Transportation and Infrastructure, June 28, 2012.

⁷⁵Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*: Prepared for the U.S. Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011).

security may be realized by allowing facilities and vessels to use a combination of traditional access control systems with the TSA background check, also known as a security threat assessment.

The findings of the study commissioned by USCG and the findings of our prior reviews of TSA's efforts to demonstrate the validity and security benefits of the TWIC program, coupled with the cost of expanding the program to include the installation of TWIC readers at ports throughout the country, raise significant concerns about the program's premise and effectiveness. While MTSA required the Secretary of Homeland Security to issue biometric transportation security cards to individuals for unescorted entry to secure areas of vessels or facilities, TSA did consider other models for implementing the TWIC program and enhancing security. However, we have found that key reasons for electing to proceed with a government-issued TWIC card have not been validated in practice. Specifically, in February 2005, TSA completed an analysis of alternatives that identified two viable models for implementing TWIC in accordance with MTSA requirements and worthy of additional consideration: (1) a federally managed option wherein the federal government would issue a credential and manage all aspects of the credentialing program except for making access control decisions at entry points to regulated operations, and (2) a federally regulated, decentralized option with a more limited federal role in which the federal government would conduct background checks and MTSA-regulated entities would be responsible for all other aspects of enrolling individuals and implementing a credential system that would comply with federal regulations.⁷⁶

The analysis of alternatives concluded that the federally managed option would best meet security needs and stated mission needs, including ensuring that (1) unauthorized individuals would be denied access to secure areas of the nation's transportation system and (2) individuals failing to maintain their eligibility requirements would have their access permissions revoked, among others. In part, these conclusions were based on the premise that the federally managed TWIC option would first establish and verify an individual's claimed identity; and once the individual's identity has been verified, it would be checked against threat

⁷⁶Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Program Analysis of Alternatives, Version 2.0*. February 15, 2005.

and background check information prior to issuing a TWIC; and once a TWIC was issued, cardholder eligibility would continue to be checked. However, in May 2011, we reported that the TWIC program was not meeting its four program goals, or mission needs, because of internal control weaknesses.⁷⁷ Among other things, we reported that internal controls in the enrollment and background checking processes were not designed to provide reasonable assurance that only qualified individuals could acquire TWICs, or once issued TWICs, TWIC holders have maintained their eligibility.

In August 2005, TSA completed an additional analysis comparing the potential costs and benefits of the two alternatives, concluding that the federally managed solution was the most economical choice because the potential benefits outweigh the costs.⁷⁸ As noted in the analysis, reasons for selecting the federally managed approach included assumptions such as the following:

- The lack of a common credential across the industry could leave facilities open to a security breach with falsified credentials.
- Under the decentralized federally regulated solution, each facility would have to perform its own background checks instead of leveraging a federal background check or security threat assessment.
- The federally managed solution would eliminate security weaknesses in existing identification systems by, among other things, having built-in security features such as sponsorship from a trusted individual or company.⁷⁹

On the basis of these assumptions, among others, TSA concluded that the federally managed alternative met 100 percent of the requirements and the federally regulated solution met only 48 percent of the requirements. The analysis further questioned whether the federal government would be able to recover costs through fees. The analysis did

⁷⁷GAO-11-657. 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.

⁷⁸Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Program Cost Benefit Analysis, Version 1.0*. August 31, 2005.

⁷⁹The TWIC program does not require sponsorship from a trusted individual or company.

not include an assessment of each alternative's technological maturity and readiness to be used as a security measure at MTSA-regulated entities without impeding commerce. However, as the TWIC reader pilot and the study commissioned by USCG demonstrate, TWIC cards and readers are not operating as envisioned.

Moreover, our reviews of the TWIC program using the federally managed option over several years, as well as other credentialing models used at airports and federal agencies, raise questions about the validity of the assumptions TSA made at the inception of the program. For example, in the airport credentialing model, the organization granting access to an individual leveraged the existing federal process for conducting background checks, and there is no requirement for a single federal security credential. The federal government is also able to recover some of the costs of the program through user fees as it is under other credentialing and endorsement models such as the Hazardous Materials endorsement for truck drivers, where applicants pay \$89.25 to have their TSA security threat assessments conducted. American Association of Airport Executives and airport operators argue that maintaining their own site-specific credentials enhances security over a standard, centrally issued credential such as TWIC and best leverages the combined local and federal knowledge for determining access decisions.⁸⁰ Likewise, federal agencies also issue their agency-specific credentials for controlling access. For example, unlike the currently implemented TWIC program, the airport and federal government's own agency-specific credentialing models intrinsically rely on organizational sponsorship, such as sponsorship by an employer, to help validate an individual's identity prior to conducting background checks to enhance security. In discussing these issues, TSA officials noted, however, that the statute as currently written requires the Secretary of Homeland Security to issue the biometric credential, and therefore decentralized issuance of the TWIC may be inconsistent with congressional intent.

⁸⁰According to DHS, a difference between the TWIC and airport credentials is that the TWIC card adheres to universally recognized security standards and is a biometric credential. However, many airport credentials are nonbiometric and in many instances do not contain an electronic chip. According to TSA, on June 8, 2006, the DHS Deputy Secretary issued a memorandum requiring that a FIPS 201-compliant card be required for TWIC production.

Furthermore, one of the driving assumptions in the TWIC cost-benefit analysis was that the lack of a common credential across the industry could leave facilities open to a security breach with falsified credentials. However, the validity of this assumption is questionable. As we reported in May 2011, our investigators conducted a small number of covert tests to assess the use of TWIC as a means for controlling access to secure areas of MTSA-regulated facilities.⁸¹ During covert tests of TWIC 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). However, our investigators did not gain unescorted access to a port where a secondary port-specific identification was required in addition to the TWIC. 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.

We have also reported that DHS had not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels.⁸² Moreover, DHS had 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. To determine if the internal control weaknesses identified in our May 2011 report still exist, we conducted limited covert testing in late 2012. Our investigators again acquired an authentic TWIC through fraudulent means and were able to use this card and counterfeit TWIC cards to access areas of ports or port facilities requiring a TWIC for entry at four ports.

In order to move forward with developing the TWIC reader rule, while this draft report was at DHS for comment, on March 22, 2013, USCG issued a notice of proposed rulemaking that would, if finalized, require owners and operators of certain MTSA-regulated vessels and facilities to use readers designed to work with TWICs.⁸³ To enhance security, the NPRM's proposed application of TWIC with electronic readers is based on, among

⁸¹[GAO-11-657](#).

⁸²[GAO-11-657](#).

⁸³78 Fed. Reg. 17,782 (Mar. 22, 2013).

other things, TWIC pilot findings, USCG's risk-based approach to categorizing vessels and facilities, and Maritime Security Risk Analysis Model (MSRAM) terrorist scenarios that could potentially be thwarted by using TWIC.⁸⁴ However, we noted the following issues in the supporting analysis.

- With regard to the TWIC pilot findings, as we previously noted, TSA did not collect data during the TWIC pilot regarding the security enhancements provided by TWIC. According to USCG, assessing security benefits was outside the scope of the TWIC pilot. We therefore cannot assess USCG's claim in its NPRM that TWIC enhances maritime security.
- The purpose of USCG's analysis for categorizing vessels and facilities into risk categories was to allocate where to place readers, not to assess the effectiveness of TWIC or determine the extent to which, or if, use of TWIC with readers would enhance security, reduce risk, or address a specific threat. Rather, USCG assumed that TWIC would help reduce the risk of a terrorist attack at a maritime facility or vessel based on the security threat assessment, but did not consider whether use of the TWIC might introduce a security risk to MTSA-regulated facilities and vessels, or whether use of TWIC would enhance the security beyond efforts already in place.
- USCG's NPRM lists three MSRAM terrorist scenarios that, according to USCG, are most likely to be mitigated by the use of TWIC readers—truck bomb, terrorist assault team, and passenger/passersby

⁸⁴The 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.

explosives/improvised explosive device.⁸⁵ According to USCG, because the function of the TWIC reader is to enhance access control, the deployment of TWIC readers would increase the likelihood of identifying and denying access to an individual attempting nefarious acts. However, USCG's preliminary analysis notes that the use of TWIC with readers would not stop terrorists from detonating a truck at the perimeter of a facility, attempting to break through the gates or protective barriers at a facility, or obtaining a TWIC card using fraudulent documents as we did through covert means. As confirmed with USCG officials, its models for assessing the benefit of TWIC do not account for these known security weaknesses. Further, USCG's draft regulatory impact analysis may lead to an overestimate (or mischaracterization) of the avoided consequences of using TWIC with readers. This is because the calculation is based on the use of TWIC with readers thwarting worst-case terrorist security incidents rather than a range of avoided consequence estimates, some of which would be lower than what was presented in the draft regulatory analysis.

While USCG has issued the TWIC-reader NPRM and has asserted benefits to be derived by using TWIC with electronic readers, USCG has not conducted an effectiveness assessment of the TWIC program, as we recommended in 2011; thus, it is unclear whether there will be sufficient time to complete the effectiveness assessment prior to the issuance of the rule. In November 2012, USCG officials reported that they are considering taking steps to assess the effectiveness of TWIC, but noted that given the complexity of the effort, the effectiveness assessment may be better suited for another organization, such as the Department of Homeland Security's Centers of Excellence, to conduct.⁸⁶ We continue to believe that the effectiveness assessment would help inform future

⁸⁵*Truck bomb*, wherein armed terrorists use a truck loaded with explosives to attack the target focal point. Under this scenario, the terrorists would attempt to overcome guards and barriers if they encounter them. *Terrorist assault team*, wherein a team of terrorists using weapons and explosives attack the target focal point. The assumption is that the terrorists have conducted prior planning and surveillance, but have no insider support of assault. *Passenger/passerby explosives/Improvised explosive device*, wherein terrorists exploit inadequate access control and detonate carried explosives at the target focal point. USCG's assumption is that the terrorists approach the target under cover of legitimate presence and are not armed. Further, for this attack mode, the terrorist is not an insider.

⁸⁶The Department of Homeland Security's Centers of Excellence is housed within DHS's Science and Technology Directorate. It is a consortium of university-based centers that organize experts and researchers to conduct multidisciplinary homeland security research and education. There are currently 12 Centers of Excellence across the country.

requirements for using TWIC with biometric card readers if the study was completed and included as part of the TWIC reader regulatory analysis. Further, given USCG's leading role in assessing and implementing security programs intended to enhance maritime security, we believe that USCG should continue to be involved in conducting this analysis.⁸⁷

Conclusions

With potentially billions of dollars needed to implement the TWIC program, it is important that DHS provide effective stewardship of taxpayer funds and avoid requiring the maritime industry to invest in a program that may not achieve its stated goals. DHS estimates that implementing the TWIC program could cost the federal government and the private sector a combined total of as much as \$3 billion over a 10-year period. This does not include an additional estimated \$234.2 million (undiscounted) to implement readers at 570 facilities and vessels that the TWIC reader NPRM currently targets. The TWIC reader pilot, conducted at a cost of approximately \$23 million, was intended to test the technology and operational impacts of TWIC cards with readers in the maritime environment. However, as a result of weaknesses in the pilot's planning, implementation, and reporting, data from the TWIC reader pilot cannot be relied upon to make decisions regarding the TWIC card reader rule or the future deployment of the TWIC program.

Additionally, the TWIC reader pilot report concluded that TWIC cards and readers provide a critical layer of security at our nation's ports. However, 11 years after initiation, the TWIC program continues to be beset with significant internal control weaknesses and technology issues, and, as highlighted in our prior and ongoing work and a related USCG report, the security benefits of the program have yet to be demonstrated. The weaknesses we have identified suggest that the program as designed may not be able to fulfill the principal rationale for the program—enhancing maritime security. Correcting technological problems with the cards and readers alone will not address the security vulnerabilities

⁸⁷USCG has primary responsibility for ensuring the safety and security of U.S. maritime interests and leading homeland security efforts in the maritime domain. In this capacity, among other things, the Coast Guard conducts port facility and commercial vessel inspections, leads the coordination of maritime information-sharing efforts, and promotes domain awareness in the maritime environment. Maritime domain awareness is the understanding by stakeholders involved in maritime security of anything associated with the global maritime environment that could adversely affect the security, safety, economy, or environment of the United States.

identified in our previous work or the USCG reports. The depth and pervasiveness of the TWIC program's planning and implementation challenges require a reassessment of DHS's efforts to improve maritime security through the issuance of a U.S. government-sponsored TWIC card and card readers. It is important that this reassessment occur before the additional investment of funds is made to install TWIC readers at the nation's ports, at considerable taxpayer expense.

Matter for Congressional Consideration

Given that the results of the pilot are unreliable for informing the TWIC card reader rule on the technology and operational impacts of using TWICs with readers, Congress should consider repealing the requirement that the Secretary of Homeland Security promulgate final regulations that require the deployment of card readers that are consistent with the findings of the pilot program. Instead, Congress should require that the Secretary of Homeland Security first complete an assessment that evaluates the effectiveness of using TWIC with readers for enhancing port security, as we recommended in our May 2011 report, and then use the results of this assessment to promulgate a final regulation as appropriate. Given DHS's challenges in implementing TWIC over the past decade, at a minimum, the assessment should include a comprehensive comparison of alternative credentialing approaches, which might include a more decentralized approach, for achieving TWIC program goals.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and DOD for review and comment. DHS provided written comments, which are printed in full in appendix V. DHS, as well as DOD, provided technical comments, which we incorporated as appropriate. In commenting on this report, DHS identified concerns with our findings and conclusions related to the use of the TWIC reader pilot results. For example, DHS asserted that the TWIC reader pilot did obtain data in sufficient quantity and quality to support the general findings and conclusions of the TWIC reader pilot report, and that the pilot obtained sufficient data to evaluate reader performance and assess the impact of using readers at maritime facilities. We disagree with this assertion. Specifically, as discussed in our report, and as confirmed by the supplemental technical comments provided by DHS, the pilot test's results were incomplete, inaccurate, and unreliable for informing Congress and for developing a regulation about the readers. For example, as discussed in the report:

-
- Installed TWIC readers and access control systems could not collect required data, including reasons for errors, on TWIC reader use, and TSA and the independent test agent did not employ effective compensating data collection measures, such as manually recording reasons for errors in reading TWICs.
 - TSA and the independent test agent did not record clear baseline data for comparing operational performance at access points with TWIC readers.
 - TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.

Moreover, in its written comments, DHS confirmed that the voluntary nature of the pilot limited opportunities for random selection of pilot sites, as we noted in our report. Therefore, the results of the pilot cannot be generalized beyond the 17 sites participating in the pilot. Further, according to DHS, we asserted that the pilot data should have been assessed using the same data collection and reporting methods for “determining the reliability of computer-processed data.” We recognize that the voluntary nature of the pilot posed challenges to the department; however, we evaluated the TWIC pilot data against recognized federal guidance for designing evaluations,⁸⁸ and *Standards for Internal Control in the Federal Government* in addition to assessing the reliability of computer-processed data.⁸⁹

Because of the significant issues we identified in this report concerning the reliability of the data collected during the pilot, when we sent the draft report to DHS for comment, we recommended that DHS not use the results collected at pilot sites on the operational impacts of using TWIC with readers to inform the upcoming TWIC card reader rule or the future deployment of the TWIC program. However, subsequent to sending the draft to DHS for comment, on March 22, 2013, USCG published the TWIC card reader NPRM, which included results from the TWIC card reader pilot. We subsequently removed the recommendation from the report, given that USCG moved forward with issuing the NPRM and incorporated the pilot results. DHS asserted that some of the perceived

⁸⁸[GAO-12-208G](#).

⁸⁹[GAO/AIMD-00-21.3.1](#); [GAO-09-680G](#).

data anomalies we cited are not significant to the conclusions TSA reached during the pilot and that the pilot report was only one of multiple sources of information available to USCG in drafting the TWIC reader NPRM. We recognize that USCG had multiple sources of information available to it when drafting the proposed rule; however, the pilot was used as an important basis for informing the development of the NPRM. Thus, we believe that the NPRM is based on findings and conclusions that are inaccurate, and unreliable for informing Congress and for developing the TWIC Card Reader Rule. In its addendum to its agency comments, DHS provides explanations for some of the weaknesses that we identified in the pilot program. We acknowledge these challenges but believe that they support our conclusion that the results of the pilot program should not be used to inform the card reader rule.

Further, related to the security benefits of the program, in its written comments, DHS maintains that a common credential used across MTSA-regulated facilities and vessels enhances security. DHS further stated that comparing airport access to maritime port access is inappropriate because most airport workers only access one airport, whereas individuals accessing maritime ports and facilities are more likely to access several different facilities. We recognize the value of conducting the security threat assessment for all workers accessing port facilities; however, TSA has not assessed the security benefits, if any, resulting from use of a common credential versus a port-, facility-, or vessel-based credential. Moreover, we continue to believe, as discussed earlier in this report, that the original assumptions that TSA made when it decided to proceed with the use of TWIC as a common credential are questionable. Thus, a comprehensive comparison of alternative credentialing approaches, which could include a more decentralized approach, would provide the necessary assurance that DHS is pursuing the most effective option for enhancing maritime security.

We are sending copies of this report to the Secretaries of Homeland Security and Defense, 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 acknowledged in appendix VI.

A handwritten signature in black ink that reads "Stephen Lord". The signature is written in a cursive style with a large initial 'S' and a large 'L'.

Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Congressional Committees

The Honorable John D. Rockefeller IV
Chairman

The Honorable John Thune
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Michael McCaul
Chairman

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

The Honorable Bill Shuster
Chairman

The Honorable Nick J. Rahall, II
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Appendix I: Objective, Scope, and Methodology

The Coast Guard Authorization Act of 2010 required that the Transportation Worker Identification Credential (TWIC) reader pilot report include (1) the findings of the pilot program with respect to key technical and operational aspects of implementing TWIC technologies in the maritime sector; (2) a comprehensive listing of the extent to which established metrics were achieved during the pilot program; and (3) an analysis of the viability of those technologies for use in the maritime environment, including any challenges to implementing those technologies and strategies for mitigating identified challenges. The act further required that we conduct an assessment of the report's findings and recommendations.¹ To meet this requirement, we addressed the following question: To what extent were the results from the TWIC reader pilot sufficiently complete, accurate, and reliable for informing Congress and the TWIC card reader rule?

To evaluate the extent to which the results from the TWIC reader pilot were sufficiently complete, accurate, and reliable for informing Congress and the TWIC card reader rule, we assessed (1) TWIC reader pilot test planning and preparation activities, (2) pilot implementation and data collection practices, and (3) the findings reported in the Department of Homeland Security's (DHS) February 2012 report to Congress on the results of the TWIC reader pilot against underlying pilot data.²

¹Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2989.

²Department of Homeland Security, *Transportation Worker Identification Credential Reader Pilot Program: In accordance with Section 104 of the Security and Accountability For Every Port Act of 2006, P.L. 109-347 (SAFE Port Act) Final Report*. February 17, 2012.

TWIC Reader Pilot Test Planning and Preparation Activities

To identify and assess TWIC reader pilot test planning and preparation activities, we reviewed our prior reports and testimonies on the TWIC program issued from September 2003 through May 2011, and key documents related to the TWIC reader pilot.³ We reviewed the following pilot planning and testing documents to understand the pilot's design and planned approach, and to assess the extent to which pilot test plans were updated and used since our November 2009 report on the subject matter.⁴

- TWIC Contactless Biometric Card and Reader Capability Pilot Test, Test and Evaluation Master Plan (TEMP), dated December 2007;
- TWIC Pilot Concept of Operations Plan, signed February 19, 2009;
- TWIC Pilot Test Reader Usage Scenarios, dated February 2, 2009;
- TWIC Initial Technical Test (ITT) Plan, signed March 20, 2009;
- TWIC Reader Functional Specification Conformance Test (F-SCT) Plan, dated March 2009;
- Naval Air (NAVAIR) Systems Command's TWIC Card Reader Environmental and Electrical Test Plan, dated February 28, 2008;
- TWIC Reader Environmental Specification Conformance Test (E-SCT) Plan, dated March 23, 2009;
- Initial Capability Evaluation Scenarios, Version 1.5, dated June 2008;
- Space and Naval Warfare Systems Command (SPAWAR), Systems Center (SSC) Atlantic, TWIC Initial Capability Evaluation Test Plan, Draft Version 1.1, dated November 13, 2008;

³GAO, *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain*, [GAO-03-1155T](#) (Washington, D.C.: Sept. 9, 2003); *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, [GAO-05-106](#) (Washington, D.C.: Dec. 10, 2004); *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, [GAO-06-982](#) (Washington, D.C.: Sept. 29, 2006); *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain*, [GAO-07-681T](#) (Washington, D.C.: Apr. 12, 2007); *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain*, [GAO-08-133T](#) (Washington, D.C.: Oct. 31, 2007); *Transportation Security: Transportation Worker Identification Credential: A Status Update*, [GAO-08-1151T](#) (Washington, D.C.: Sept. 17, 2008); *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); and *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-10-43](#).

- TWIC Baseline Data Collection Plan, dated January 2009;
- TWIC Early Operational Assessment (EOA) Test Plan, signed March 18, 2009; and
- TWIC Reader Pilot Program System Test and Evaluation (ST&E) Test Plan, dated February 2010 (signed August 4, 2011).

We further reviewed the TWIC Reader Pilot Program Data Analysis Plan, dated October 2010. The plan was developed in response to our November 2009 recommendations to develop an evaluation plan and data analysis plan to identify pilot data to be collected and associated data collection approaches.⁵ We also recommended that the evaluation plan identify areas for which the TWIC reader pilot would not provide the information needed to report to Congress and implement the TWIC card reader rule, and document the compensating information to be collected and an approach for obtaining and evaluating the information obtained through this effort. We assessed the extent to which the TWIC Data Analysis Plan addressed our 2009 recommendations and the extent to which it was used during the pilot. We also reviewed the extent to which two studies commissioned by the U.S. Coast Guard (USCG) addressed our 2009 recommendations.⁶

To further understand TWIC reader pilot planning activities, we reviewed actions taken to ensure that the TWIC card and reader technology used during the pilot would function properly prior to being fielded at pilot sites. First, we reviewed steps taken by the Transportation Security Administration (TSA) to assess the durability of the finalized TWIC card, which is to be used in the harsh maritime environment. We compared these steps against steps taken by the Department of Defense, which also utilizes credentials that are exposed to harsh environments, and the results of our prior work on credential durability at the State Department.⁷ Second, we reviewed TSA's approach to testing and assessing the

⁵[GAO-10-43](#).

⁶Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, a report prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011). Booz, Allen, Hamilton. *Port Facility Congestion Study, United States Coast Guard*, a report prepared for the United States Coast Guard, (McLean, Virginia: February 16, 2011).

⁷See GAO, *Border Security: Improvements in the Department of State's Development Process Could Increase the Security of Passport Cards and Border Crossing Cards*, [GAO-10-589](#) (Washington, D.C.: June 1, 2010).

readiness of readers for use during the pilot. Specifically, we considered TSA's modified approach for testing and assessing reader readiness prior to use at pilot sites as well as the results of the more detailed environmental and functional reader testing conducted. We further reviewed reader testing plans and results to identify and assess the performance criteria used to determine whether tested readers would severely impact pilot site operations or prevent the collection of useful pilot data.

TWIC Reader Pilot Data Collection Practices

To identify and assess the pilot as implemented, we reviewed relevant legislation, such as the Maritime Transportation Security Act of 2002 (MTSA),⁸ amendments to MTSA made by the Security and Accountability For Every Port Act of 2006 (SAFE Port Act),⁹ and the Coast Guard Authorization Act of 2010¹⁰ to inform our review of requirements for TWIC and the TWIC reader pilot specifically. We further reviewed key TWIC reader pilot test documents, such as the TWIC reader pilot test and evaluation master plan and underlying test protocols, and compared planned pilot testing and data collection practices with the methods used to collect and analyze pilot data. In doing so, we reviewed and assessed the following documents where TWIC reader pilot results were recorded.

- TWIC Reader Pilot Program Baseline Report, dated December 2010;
- TWIC Initial Technical Test Report, dated September 2010;
- TWIC Card Reader Environmental Specification Conformance and Evaluation Test, signed March 2, 2010;
- TWIC Reader Pilot Program TWIC Early Operational Assessment Summary Report, signed February 6, 2012;
- Early operational assessment reports (final reports) provided by TSA and the independent test agent for each of the 17 pilot sites;
- TWIC Reader Pilot Program System Test and Evaluation Summary Report, signed February 6, 2012;
- Systems test and evaluation reports (ST&E) (final reports) provided by TSA and the independent test agent for each of the 17 pilot sites;
- 117 pilot site trip reports where on-site observations were recorded against data recorded in final EOA and ST&E reports;

⁸Pub. L. No. 107-295, 116 Stat. 2064.

⁹Pub. L. No. 109-347, 120 Stat. 1884.

¹⁰Pub. L. No. 111-281, 124 Stat. 2905.

- TWIC Reader Pilot Program Data Analysis Plan, dated October 2010;
- 46 TWIC Program Weekly and Monthly Status Reports provided by the independent test agent; and
- TSA's TWIC Reader Pilot Cost Summary Report by Participant.

We further assessed TWIC reader pilot data collection efforts against established practices for designing evaluations, assessing the reliability of computer-processed data, as well as internal control standards for collecting and maintaining records.¹¹ To do so, we identified practices in place and assessed whether measures and internal controls were in place to ensure the resulting data were sufficiently complete, accurate, and reliable. We further interviewed officials representing 14 of the 17 participating pilot sites, the independent test agent (SPAWAR) and relevant agency officials that oversaw or contributed to the pilot results at TSA and USCG about pilot testing approaches, results, and challenges.¹² While information we obtained from the interviews with officials representing 14 of the 17 participating pilot sites may not be generalized across the maritime transportation industry as a whole, because we selected TWIC reader pilot participants located across the nation and representing varying maritime operations, the interviews provided us with information on the views of individuals and organizations that participated in the pilot and could be directly affected by TWIC reader use requirements. We also reviewed pilot site reports and underlying data to assess the extent to which data in these reports were collected and assessed in a consistent and complete manner, so as to ensure the data and the analysis thereof could result in accurate and reliable findings. TSA reported that it relied on each of the final EOA and ST&E reports for each of the 17 pilot sites—a total of 34 reports—as the basis of its report to Congress. Accordingly, we tested the data in each of the 34 reports as follows.

1. We requested that TSA and the independent test agent each provide us with final copies of each pilot site's EOA and ST&E pilot site

¹¹GAO, *Designing Evaluations: 2012 Revision*, [GAO-12-208G](#) (Washington, D.C.: Jan. 2012); *Assessing the Reliability of Computer Processed Data*, [GAO-09-680G](#) (Washington, D.C.: July, 1, 2009); and [GAO/AIMD-00-21.3.1](#), *Standards for Internal Control in the Federal Government* (Washington, D.C.: November 1999).

¹²We met with officials representing pilot participants at the Port of Long Beach; Port of Los Angeles; Port Authority of New York and New Jersey; Clipper Navigation, in Seattle, Washington; Staten Island Ferry in Staten Island, New York; and Watermark Cruises in Annapolis, Maryland.

reports. We compared the 34 reports provided by TSA with the 34 reports provided by the independent test agent to validate whether the final reports provided by each entity were identical. We also reviewed the 117 pilot site trip reports provided by TSA and the independent test agent. Pilot site trip reports documented observations made by TSA or the independent test agent during visits to each pilot site and were to serve as input to the final EOA and ST&E pilot site reports. Of the 117 pilot site trip reports, 76 contained access point throughput data. We further reviewed 34 of 76 pilot site trip reports to identify the extent to which all collected observations and data were included in the final EOA and ST&E pilot site reports, and to determine if reasons for exclusions, if any, were documented.¹³ While information we obtained from our review of the 34 pilot site trip reports compared with the final EOA and ST&E pilot site reports cannot be generalized, the reports provided us with important insight on potential limitations present in reported pilot data.

2. We employed computer-based testing techniques, including the development of a database, to assess the completeness of collected data as well as the consistency of data collected across pilot sites. To do so, we used TWIC reader pilot data results recorded in the TWIC Reader Pilot Program Baseline Report and the 34 final EOA and ST&E pilot site reports. We linked results reported in the baseline report and each pilot site's EOA or ST&E reports where data were present for a particular pilot site, access point, and reader. These techniques provided us with the following summary and comparative views of collected pilot data, among others, which in part served as the basis of our data analysis:
 - compiled data by pilot site;
 - compiled data on baseline population of users at each pilot site and reported access points;
 - comparison of the total population at baseline to total population reported during the ST&E phase;
 - view of pilot site access point and reader matches across testing results (baseline data, Systems Operational Verification Testing (SOVT) data, EOA data, and ST&E data);
 - view of tested reader and access control system characteristics;

¹³We selected the 34 pilot site trip reports because they represented nearly half of all trip reports containing throughput data and belonged to six pilot participants located in the north east and southern United States..

-
- comparison of baseline throughput times versus EOA and ST&E throughput times for access points with similar readers used;
 - comparison of data across the pilot to identify trends, if any, in areas such as risk level, facility and vessel type, access point type, access decision location, testing mode throughput and transactions, reader hardware model and software version, reader types (fixed versus portable), interface type (contact versus contactless), communication protocol, whether or not registration was used, the enrollment process, the source of the biometric reference template, and canceled card list input frequency by site;
 - comparison of the total number of access points identified during baseline data collection versus the total of access points tested during the EOA and ST&E phases of the pilot;
 - comparison of the mean, median, and mode based on the ST&E number of throughput transactions; and
 - assessment of testing duration during EOA and ST&E testing phases for both throughput and transaction data collection efforts.

We utilized the results of our above-noted testing techniques and data results recorded in the TWIC Reader Pilot Program Baseline Report and the 34 final EOA and ST&E pilot site reports to inform our analysis of the pilot data's completeness, reliability, and accuracy. We further reviewed the data with TSA—the agency leading the TWIC reader pilot—and the independent test agent to better understand observed anomalies. We also considered input from pilot site officials regarding the testing operations and officials from USCG who contributed to the TWIC reader pilot or are to utilize the results of the pilot to inform their future implementation of TWIC. Last, we reviewed the two reports commissioned by USCG to inform the impending regulation on the use of TWIC cards with biometric readers in consideration of comparative data.¹⁴

DHS's TWIC Reader Pilot Report to Congress

We analyzed and compared the TWIC reader pilot data with DHS's TWIC reader pilot report submitted to Congress to determine whether the findings identified in the report are based on sufficiently complete,

¹⁴Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, a report prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011). Booz, Allen, Hamilton. *Port Facility Congestion Study, United States Coast Guard*, a report prepared for the United States Coast Guard, (McLean, Virginia: February 16, 2011).

accurate, and reliable evidence, and are supported by pilot documentation. In doing so, we leveraged our above-noted assessments of TWIC reader pilot planning and data collection practices. Since our assessment determined that pilot data on TWIC technology and operational performance at pilot sites were incomplete, inaccurate, or unreliable, we did not further report on differences between TWIC reader pilot data and DHS's TWIC reader pilot report. We focused the remainder of our assessment on three areas that were not identified in our prior analysis: (1) reported costs and statements about cost savings, (2) reported entry times for accessing pilot sites versus reader response times, and (3) statements of enhanced security resulting from the use of TWIC with biometric readers.

- **Reported costs and cost savings.** We sought to validate the cost data reported in DHS's TWIC reader pilot report to Congress against cost data provided by TSA and the independent test agent. We reviewed cost data in the report and compared them with the cost schedule provided by TSA that, according to TSA, served as the central cost data document used in support of the data reported to Congress. We further compared the data in the report to Congress against the data held in individual pilot site reports. In addition, we compared the data in TSA's central cost data document with cost data in each individual EOA and ST&E pilot site report to assess the extent to which cost data in each matched. We reviewed our prior work and received input from seven pilot participants regarding their planned implementation of TWIC readers and related systems. This enabled us to assess the extent to which costs reported in DHS's report represented likely costs for fully implementing, operating, and maintaining the use of TWIC with readers at these pilot sites. Last, we reviewed available pilot documentation to identify data demonstrating that cost savings had been realized as a result of implementing the use of TWIC with biometric card readers. We further reviewed the results of a report commissioned by the Coast Guard to inform the impending regulation on the use of TWIC cards with biometric readers.¹⁵
- **Reported entry time for accessing pilot sites versus reader response time.** We reviewed DHS's TWIC Reader Pilot Program

¹⁵Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, a report prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011).

report to Congress to assess the presentation of recorded time measurements. Specifically, we assessed the extent to which the report accurately conveyed entry time for accessing piloted sites, known as throughput time, versus reader response time, known as transaction time. We further assessed the reported time data to identify the extent to which, if at all, throughput time and transaction time data were used interchangeably, could be validated against data from the pilot, and representations made about the data could be validated by data collected during the pilot.

- **Enhanced security.** We reviewed DHS's TWIC Reader Pilot Program report to Congress and identified statements made about security enhancements based on pilot results. We examined available pilot documentation to identify data demonstrating that security at the piloted sites had been realized as a result of implementing the use of TWIC with biometric card readers. We further discussed the lack of supporting pilot data with TSA and DHS and provided opportunities for data to be provided. We also reviewed statements made by DHS officials during a hearing before Congress on the results of the pilot and the results of a report commissioned by USCG to inform the impending regulation on the use of TWIC cards with biometric readers.¹⁶ We further considered two key documents, the TWIC Program Analysis of Alternatives and the TWIC Program Cost Benefit Analysis,¹⁷ which were used to support the decision to execute the TWIC program to enhance security using common credential and biometric card readers. In doing so, we assessed the information presented in the documents and the operational cost and security benefits defined therein as having significant weight on the decision to implement the TWIC program through the use of a federally issued

¹⁶U.S. Department of Homeland Security, Joint Written Statement of Kelli Ann Walther, Acting Deputy Assistant Secretary, Screening Coordination Office, Office of Policy, and Rear Admiral Joseph Servidio, Assistant Commandant for Prevention Policy, U.S. Coast Guard, Before the House Committee on Transportation and Infrastructure, June 28, 2012. Systems Planning and Analysis, Inc. *Survey of Physical Access Control System Architectures, Functionality, Associated Components, and Cost Estimates*, a report prepared for the United States Coast Guard Office of Standards Evaluation and Development (CG-523), (Alexandria, Virginia: March 31, 2011). Booz, Allen, Hamilton. *Port Facility Congestion Study, United States Coast Guard*, a report prepared for the United States Coast Guard, (McLean, Virginia: February 16, 2011).

¹⁷Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Program Analysis of Alternatives*, Version 2.0. February 15, 2005. Transportation Security Administration. *Transportation Worker Identification Credential (TWIC) Program Cost Benefit Analysis*, Version 1.0. August 31, 2005.

credential and biometric card readers. We then assessed the defined security benefits against our 2011 review of the TWIC program's security as implemented¹⁸ and subsequent actions taken by TSA and USCG to address recommendations made in the product. Our investigators also conducted limited covert testing of TWIC program internal controls for acquiring and using TWIC at four maritime ports to update our understanding of the effectiveness of TWIC at enhancing maritime security since our work in May 2011.¹⁹ The information we obtained from covert testing efforts is not generalizable, but we believe that the information from our covert tests provided us with important additional perspective and context on the TWIC program. Finally, we reviewed and assessed the security benefits presented in the TWIC reader notice of proposed rulemaking (NPRM) issued March 22, 2013, to determine whether the effectiveness of the noted security benefits was presented.

We conducted this performance audit from January 2012 to May 2013 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 objective. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

¹⁸ [GAO-11-657](#).

¹⁹The four ports tested as part of this limited covert testing update were selected because (1) we conducted covert testing at these locations during our prior review, and (2) they were geographically dispersed across the United States, representing the east coast, south, and southwest.

Appendix II: Key TWIC Implementation Actions

Table 3 summarizes key TWIC program laws and milestones for implementing the program through November 2012.

Table 3: Key Transportation Worker Identification Credential (TWIC) Program Laws and Implementation Actions from November 2002 through November 2012

Date	Key TWIC implementation actions
November 2002	Enactment of the Maritime Transportation Security Act (MTSA) of 2002, which 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. ^a
August 2004 through August 2005	As part of its prototype testing, the Transportation Security Administration (TSA)—through a private contractor—tested the TWIC program at 28 transportation facilities across the country from August 2004 through June 2005. TSA also completed an analysis of alternatives and a cost-benefit analysis in February and August 2005 that considered alternatives for implementing TWIC in accordance with MTSA. TSA concluded that implementing TWIC as a federally managed program wherein TSA issued a single federal credential would best enhance security.
August 2006	TSA decided that the TWIC program would be implemented in the maritime sector using two separate rules. The credential rule covers use of TWICs as a credential for gaining access to facilities and vessels. The second rule, the TWIC card reader rule, is planned to address the use of access control technologies, such as biometric card readers, for confirming the identity of the TWIC holder against the biometric information on the TWIC.
October 2006	The Security and Accountability For Every Port Act of 2006 directed the Secretary of Homeland Security to, among other things, implement the TWIC program at the 10 highest-risk ports by July 1, 2007, and to conduct a pilot program to test TWIC access control technologies, such as TWIC readers, in the maritime environment. ^b
January 2007	TSA and the U.S. Coast Guard (USCG) issued the credential rule requiring worker enrollment in the TWIC program and TWIC issuance. ^c TSA also awarded a contract to begin enrolling workers and issuing TWICs to workers.
June 2008	As part of the TWIC reader pilot, TSA issued an agency announcement calling for biometric card readers to be submitted for assessment as TWIC readers.
August 2008	TSA initiated the TWIC reader pilot testing, starting with the initial capability evaluation of TWIC readers.
April 2009	On April 15, 2009, all captain of the port zones nationwide began compliance with TWIC requirements. ^d
September 2010	The Coast Guard Authorization Act of 2010 required that the findings of the TWIC reader pilot be included in a report to Congress, and that we assess the reported findings and recommendations. ^e
May 31, 2011	TSA completed the TWIC reader pilot.
February 27, 2012	DHS delivered its report on TWIC reader pilot results to Congress.
November 16, 2012	DHS submitted a draft Notice of Proposed Rulemaking on TWIC reader requirements to the Office of Management and Budget for review.

Source: GAO summary of TWIC program activities and requirements.

^aPub. L. No. 107-295, § 102(a), 116 Stat. 2064, 2073 (codified at 46 U.S.C. § 70105).

^bPub. L. No. 109-347, § 104(a), 120 Stat. 1884, 1888 (codified at 46 U.S.C. § 70105(i), (k)).

^c72 Fed. Reg. 3492 (Jan. 25, 2007).

^dA Captain of the Port Zone is a geographic area for which a Coast Guard captain of the port retains authority with regard to enforcement of port safety, security, and marine environmental protection regulations.

^ePub. L. No. 111-281, § 802, 124 Stat. 2905, 2989.

Appendix III: TWIC Program Funding

From fiscal year 2002 through fiscal year 2012, the TWIC program had funding authority totaling \$393.4 million, including \$111.4 million in appropriated funds (including reprogramming and adjustments).¹ An additional \$151.3 million has been made available to maritime facility and vessel owners and operators through port and transportation security grants related to TWIC.² Table 4 provides further funding details.

Table 4: Transportation Worker Identification Credential (TWIC) Program Funding from Fiscal Years 2002 through 2012

Dollars in millions

Fiscal year	Appropriated	Reprogramming	Adjustments	TWIC fee authority ^a	Federal security grant awards related to TWIC	Total funding authority including security grants
2002	0	0	0	0	0	0
2003	\$25.0	0	0	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	3.9	\$4.7	\$10.0	31.5 ^b	50.1
2008	8.1	0	0	42.5	18.0	68.6
2009	0	0	0	109.3	22.2 ^c	131.5
2010	0	0	0	45.0	15.7	60.7
2011	0	0	0	45.0	23.3	68.3
2012	0	0	0	30.2	16.3	46.5
Total	\$87.8	\$18.9	\$4.7	\$282.0	\$151.3	\$544.7

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

^aFigures in the TWIC fee authority column represent the dollar amount the Transportation Security Administration (TSA) is authorized to collect from TWIC enrollment fees and not the actual dollars collected. TSA reports to have collected a total of \$207.2 million through its fee authority, \$41.7 million for fiscal year 2008, \$76.2 million for fiscal year 2009, \$30.6 million for fiscal year 2010, \$26.5 million for fiscal year 2011, and \$32.2 million for fiscal year 2012.

^bFederal 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.

¹An additional \$282 million in funding was authorized in fiscal years 2007 through 2012 through the collection of TWIC enrollment fees by TSA, and \$23.03 million had been made available to pilot participants from the Federal Emergency Management Agency (FEMA) grant programs—the Port Security Grant Program and the Transit Security Grant Program.

²Sixteen of 17 pilot sites participating in the pilot were funded using these grants.

²Federal 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 funding. See Pub. L. No. 111-5, 123 Stat. 115 (2009).

As reported by DHS, the TWIC reader pilot cost approximately \$23 million and was funded by appropriated funds and federal security grant awards.³ 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, as the credential rule did not require the installation or use of TWIC cards with readers. The notice of proposed rulemaking published on March 22, 2013, estimated an additional cost of \$234.2 million (undiscounted) to implement readers at 570 facilities and vessels that the TWIC reader currently targets.⁴

³Over \$23 million had been made available to pilot participants from two FEMA grant programs—the Port Security Grant Program and the Transit Security Grant Program. Of the \$23 million, grant recipients agreed to spend nearly \$15 million on the TWIC reader pilot. However, DHS is unable to validate the exact amount grant recipients spent on the TWIC reader pilot, as rules for allocating what costs would be included as TWIC reader pilot costs versus other allowable grant expenditures were not defined. Sixteen of 17 pilot sites participating in the pilot were funded using these grants. In addition, TSA obligated an additional \$8.1 million of appropriated funds to support the pilot.

⁴A notice of proposed rulemaking is published in the *Federal Register* and contains notices to the public of the proposed issuance of rules and regulations.

Appendix IV: TWIC Reader Pilot Sites, Locations, and Types of Maritime Operation or Industry Group

	Location	Participant name	Type of maritime operation or industry group
1	Annapolis, Maryland	Watermark Cruises	Small passenger vessel/towboat/other
2	Brownsville, Texas	Port of Brownsville	Container terminal
3	Port Authority of New York/New Jersey	APM Terminal	Container terminal
4	Port Authority of New York/New Jersey	Maher Terminal	Container terminal
5	Port Authority of New York/New Jersey	Brooklyn Marine Terminal	Container terminal
6	Port of Long Beach	BP	Petroleum facilities
7	Port of Long Beach	Metropolitan Stevedore Company	Break-bulk
8	Port of Long Beach	Total Terminals International	Container terminal
9	Port of Long Beach	Sea Launch	Small passenger vessel/towboat/other
10	Port of Long Beach	SSA Marine	Container terminal
11	Port of Los Angeles	NuStar Energy	Petroleum facilities
12	Port of Los Angeles	World Cruise Center	Large passenger vessel / terminal
13	Port of Los Angeles	APL	Container terminal
14	Norco, Louisiana	Shell Chemical LP	Petroleum facilities
15	Seattle, Washington	Clipper Navigation	Small passenger vessel/towboat/other
16	Staten Island, New York	Staten Island Ferry	Small passenger vessel/towboat/other
17	Vicksburg, Mississippi	Magnolia Marine Transport	Small passenger vessel/towboat/other

Source: DHS TWIC card reader report to Congress.

Appendix V: Comments from the Department of Homeland Security

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



**Homeland
Security**

April 17, 2013

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

Re: Draft Report GAO 13-198, "TRANSPORTATION WORKER IDENTIFICATION
CREDENTIAL: Card Results Are Unreliable; Security Benefits Need to Be Reassessed"

Dear Mr. Lord:

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

We are concerned that the GAO report does not provide a complete picture of the context and perspective the U.S. Coast Guard (USCG) considered when deciding how to use the results of the Transportation Worker Identification Credential (TWIC) reader pilot during the development of the recent TWIC reader rulemaking.¹ GAO asserts that the card reader pilot data should have been assessed using the same data collection and reporting methods for determining the reliability of computer-processed data. Adhering to such standards would require test conditions beyond our control in the TWIC card reader pilot. GAO envisioned a test environment that DHS was unable to establish for many reasons, not the least of which was the voluntary nature of the pilot. Also there were limited fiscal and workforce resources made available at participating sites, and extreme differences in the nature of operations among affected maritime facilities. TSA's interest in covering a wide range of operations, conditions, and entities, as required by statute and the need to avoid interfering with daily operations at participating pilot sites, affected data collection.

Moreover, the perceived data anomalies GAO discussed in the report are not significant to the conclusions TSA reached during the pilot. The USCG understood early on the limitations inherent in a voluntary participation pilot and sought out additional sources for data that could be used in the development of the rulemaking. In the attached document, we discuss and respond in detail to GAO's assertions concerning data integrity and validity.

¹ 78 Fed. Reg. 17782 (March 22, 2013).

Value of the TWIC Program

GAO asserts that DHS must reassess the security benefits of the TWIC program. DHS continues to evaluate the security benefits of the TWIC program, as well as areas in need of improvement for future action. It is important to understand the security value the TWIC program brings to the maritime industry. USCG is the primary DHS Component responsible for access control in the maritime industry. The TWIC program is an integral and very important part of our Nation's layered maritime security system. The program affords a level of vetting and identity management never before possible. TWIC provides a uniform, industry-wide, biometric, tamper-resistant credential that is issued following successful completion of the security threat assessments (STAs)². Currently, USCG requires maritime operators to visually inspect the TWIC before granting access to controlled locations on board vessels and at facilities. Use of this common credential enables federal, state, tribal, and local law enforcement entities to verify the identity of individuals and their eligibility to enter secure areas with a level of confidence that was not feasible prior to TWIC, when potentially thousands of different licenses and facility credentials were accepted for entry. Use of a common credential, such as the TWIC, will serve as a vital enabler for the future, as risk-based access control decisions and intelligence capabilities mature.

TSA uses the identity verification and enrollment standards created by the Department of State to issue passports, trained enrollment personnel, and score each applicant's identity documents during enrollment using electronic fraud detection software used to score each applicant's identity documents during enrollment. Since October 2007, TSA has conducted STAs of more than 2.5 million workers who seek unrestricted access to secure areas of maritime facilities. In that time, TSA has determined that approximately 50,000 individuals do not meet the security standards established by Congress in the Maritime Transportation Security Act of 2002 (MTSA)³ and implemented by TSA through rulemaking.⁴

USCG recently published a notice of proposed rulemaking (NPRM) on TWIC readers,⁵ in which use of TWIC readers would be required for certain higher-risk vessels and facilities. The proposed rule would further enhance security by providing an additional verification of the TWIC card and of the owner's identity. TWIC readers determine whether: the card is authentic, the card was issued by TSA, and not a clone; the card has expired; and the card has been revoked or reported lost or stolen. When used in the biometric mode, cards and readers additionally confirm through a biometric fingerprint match that the person using the card is the rightful owner of the card. When combined, the TWIC card and reader can perform these additional checks virtually anywhere with portable or fixed readers because connectivity to a database is not required.

² TSA conducts a check of criminal history, immigration, and terrorism records for each TWIC applicant, as well as a daily terrorist check of each TWIC holder.

³ Public Law 107-295 (November 25, 2002), codified at 46 U.S.C. 70105.

⁴ 72 Fed. Reg. 3492 (January 25, 2007), codified at 49 C.F.R. part 1572.

⁵ 78 Fed. Reg. 17782 (March 22, 2013).

Oversight of Program Challenges

In the past year, four major challenges impacting the TWIC program have converged: 1) the expiration of 1.5 million TWICs over an 18-month period with the resultant demand for re-enrollments and replacement cards; 2) development and publication of USCG's reader NPRM; 3) realignment of the TWIC system to comply with the new congressional mandate to limit enrollment and card issuance to one visit; and 4) transition of the program from the current single-provider contract to separate contracts for enrollment services and system operation.

As a result of these challenges, DHS established a working group to better understand current concerns about the TWIC program and to assess the potential benefits and challenges of requiring reader use. Following a series of port visits to identify potential improvements to the administration of the TWIC program, DHS leadership prioritized the following activities to enhance the program: 1) substantially enhance customer service; 2) review standards-based smart card technology; 3) overhaul administration of the TWIC program; and 4) ensure successful and seamless transition among contractors. To facilitate this effort, DHS initiated a program evaluation through a formal DHS Acquisition Review Board (ARB) that met on March 28, 2013, and will continue to meet on a regular basis. The intent of this ARB is to address the aforementioned challenges.

Path Forward

At the direction of Congress and Department leadership, beginning this summer, TSA will embark on the first phase of an initiative with a test in Alaska to allow individuals to apply for and obtain a TWIC with one visit to an enrollment center. To improve the customer experience, the "OneVisit" initiative would expand nationwide in 2014. This represents the most significant program change since TWIC's inception and will greatly ease the burden on future applicants seeking a TWIC. Under OneVisit, applicants will visit an enrollment center to enroll and, upon completion of a satisfactory STA, a card will be produced and mailed directly to the applicant. OneVisit will provide applicants greater flexibility in getting a TWIC and also ease congestion at enrollment centers by eliminating subsequent visits currently required to activate the card and select a PIN.

We are planning additional customer service improvements:

- Expanding the number of TWIC enrollment centers. TSA's new Universal Enrollment Services (UES) contract will increase the number of TWIC enrollment centers to more than 300 sites throughout the United States.
- Implementing a robust oversight effort to gauge sustained customer service at our enrollment centers.
- Developing a Web-based process to apply for Extended Expiration Date TWICs or replacement cards. This will enable current TWIC holders to bypass calling the TWIC call center to make these requests, and make them at their convenience over the Internet.

- Increasing mobile enrollment opportunities. The UES contract will require the contractor to provide mobile enrollment services to facilities that want to enroll workers on-site. This contract requirement will better define the requirements for mobile enrollments.

TSA established a Qualified Technology List (QTL) process to provide MTSA-regulated facility owners and operators with a list of TWIC readers that meet the TWIC specification and therefore comply with the proposed requirements in the TWIC reader NPRM. On November 1, 2012, TSA announced the availability of three laboratories in the National Voluntary Laboratory Accreditation Program accredited to certify readers for compliance with the TWIC card and reader specification. Prior to the announcement, TSA worked with National Institute of Science and Technology, independent laboratories, and the reader industry to provide QTL workshops and test cards to all interested parties. The QTL process provides the reader industry with a formal, repeatable, standardized approach for certifying readers and reporting the results to TSA. Once each reader is certified, TSA will update the publicly available QTL with information on the new reader. TSA and USCG held an Industry Day event on April 15, 2013, to update reader vendors on the reader NPRM and answer questions about the QTL process. The recent publication of the reader rule NPRM is expected to spur further interest and reader development.

The draft report contained one recommendation with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation: Not use the results collected at pilot sites on the operational impacts of using TWIC to inform the upcoming TWIC card reader rule or the future deployment of the TWIC program.

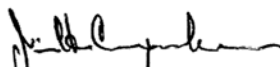
Response: DHS concurs and notes that the card reader pilot results are not the sole basis for the TWIC reader NPRM, nor for the direction we take with the TWIC program in the future. Because of the testing conditions endemic to a voluntary pilot program, TSA encountered many challenges in the implementation of the TWIC reader pilot but did obtain considerable data in sufficient quantity and quality to support the general findings and conclusions of the TWIC reader pilot report. The pilot obtained sufficient data to evaluate reader performance and assess the impact of using readers at maritime facilities.

We believe the card reader pilot produced valuable information concerning the environmental, operational, and fiscal impacts of the use of TWIC readers for use in the development of the reader NPRM. The regulatory analysis for the TWIC reader NPRM accounts for maintenance, replacement, and operation costs of readers in addition to the costs reported in the TWIC pilot study, contrary to GAO's assertions. As both the TWIC pilot report and GAO's review note, not all facilities implemented readers at all access points during the pilot in the same manner they will in the future in order to meet finalized regulatory requirements. In the regulatory analysis for the TWIC reader rule, for example, USCG estimated the number of access points per facility, by facility type through the use of an independent data source (Facility Security Plans). This independent data supplemented what was learned through the TWIC pilot and helped account for TWIC reader implementation at all access points when developing the proposed rule.

TWIC reader systems function properly when they are designed, installed, and operated in a manner consistent with the characteristics and business needs of the facility or vessel operation. The analysis for the pilot also concluded that reader systems can make access decisions efficiently. The key is recognizing the business needs and characteristics of the facility or vessel and ensuring that the reader place supports those needs. These conclusions and other information in the pilot report allowed the report to be one of multiple sources of information available to USCG in drafting the TWIC reader NPRM that was published on March 22, 2013. Additionally, we will use pertinent information we receive during the public comment period from the public and affected parties to further evaluate further reader use and performance. We believe GAO's final report would be enhanced by reviewing the NPRM and regulatory assessment. The attachment identifies other areas of enhancements.

Again, thank you for the opportunity to review and provide comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Attachment

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

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

Acknowledgments

In addition to the contact named above, David Bruno (Assistant Director), Joseph P. Cruz (Analyst-in-Charge), David Alexander, Hiwotte Amare, Nabajyoti Barkakati, Chuck Bausell, Justin Fisher, Tracey King, James Lawson, Lara Miklozek, and Anna Maria Ortiz made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

