

November 2009

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

Accountability * Integrity * Reliability



Highlights of [GAO-10-43](#), a report to congressional requesters

Why GAO Did This Study

The Transportation Worker Identification Credential (TWIC) program, which is managed by the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and the U.S. Coast Guard, requires maritime workers who access secure areas of transportation facilities to obtain a biometric identification card to access these facilities. A federal regulation set a national compliance deadline of April 15, 2009. TSA is conducting a pilot program to test the use of TWICs with biometric card readers in part to inform the development of a second TWIC regulation. GAO was asked to evaluate TSA's and the Coast Guard's progress and related challenges in implementing TWIC, and to evaluate the management challenges, if any, TSA, Coast Guard, and DHS face in executing the TWIC pilot test. GAO reviewed TWIC enrollment and implementation documents and conducted site visits or interviewed officials at the seven pilot program sites.

What GAO Recommends

Among other things, GAO recommends that TSA expedite the development of contingency and disaster recovery plans and system(s), and TSA and Coast Guard develop a detailed evaluation plan to help ensure that needed information on biometrics will result from the pilot. DHS generally concurred and discussed actions to implement the recommendations, but these actions will not fully address the intent of all of the recommendations.

[View GAO-10-43 or key components.](#)

For more information, contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov.

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers

What GAO Found

TSA, Coast Guard, and the maritime industry took a number of steps to enroll 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million users, by the April 15, 2009, national compliance deadline, but experienced challenges that resulted in delays. TSA and the Coast Guard implemented a staggered compliance approach whereby each of 42 regions impacted by TWIC were required to meet TWIC compliance prior to the national compliance date. Further, based on lessons learned from its early experiences with enrollment and activation, and to prepare for an expected surge in TWIC enrollments and activations as compliance dates approached, TSA and its contractor increased the number of stations available for TWIC enrollment and activation. While 93 percent of users were enrolled in TWIC by the compliance date, TSA data shows that some workers experienced delays in receiving TWICs. Among reasons for the delays, a power failure in October 2008 occurred at the government facility that processes TWIC data. The power failure resulted in credential activations being halted until late November 2008, and the inability to set new personal identification numbers (PIN) on 410,000 TWICs issued prior to the power failure. While TSA officials stated that they are taking steps to develop a disaster recovery plan by next year and a system to support disaster recovery by 2012, until such a plan and system(s) are put in place, TWIC systems remain vulnerable to similar disasters. While the full cost of this power failure is unknown, based on TSA provided figures, it could cost the government and industry up to approximately \$26 million to replace all affected TWIC cards.

While TSA has made progress in incorporating management best practices to execute the TWIC pilot, TSA faces two management challenges in ensuring the successful execution of the pilot test aimed at informing Congress and the development of the second TWIC regulation. First, TSA has faced challenges in using the TWIC pilot schedule to guide the pilot and accurately identify the pilot's completion date. TSA has improved its scheduling practices in executing the pilot, but weaknesses remain, such as not capturing all pilot activities in the schedule, that may adversely impact the schedule's usefulness as a management tool and for communicating with pilot participants in the maritime industry. Second, shortfalls in TWIC pilot planning have hindered TSA and Coast Guard's efforts to ensure that the pilot is broadly representative of deployment conditions and will yield the information needed—such as information on the operational impacts of deploying biometric card readers and their costs—to accurately inform Congress and the second rule. This is in part because these agencies have not developed an evaluation plan that fully identifies the scope of the pilot and specifies how the information from the pilot will be analyzed. The current evaluation plans describe data collection methods but do not identify the evaluation criteria and methodology to be used in analyzing the pilot data once collected. A well-developed, sound evaluation plan would help TSA and the Coast Guard determine how the data are to be analyzed to measure the project's performance.

Contents

Letter		1
	Background	7
	TSA, Coast Guard, and the Maritime Industry Implemented a Number of Measures to Facilitate Enrollment, Activation, and Compliance but Implementation Efforts Were Affected by the Lack of Planning for Potential System Failures	13
	Challenges in Program Scheduling and Evaluation May Hinder the TWIC Reader Pilot's Usefulness	25
	Conclusions	45
	Recommendations for Executive Action	47
	Agency Comments and Our Evaluation	48
Appendix I	Objectives, Scope, and Methodology	53
Appendix II	Key TWIC Implementation Actions	59
Appendix III	Phased-In Captain of the Port Zone Compliance Schedule (Revised February 19, 2009)	60
Appendix IV	Scheduling Best Practices	61
Appendix V	Assessment of the TWIC Pilot against the Potential TWIC Requirements under Consideration in the March 27, 2009, TWIC Advanced Notice of Proposed Rulemaking for the Card Reader Rule	63
Appendix VI	Comments from the Department of Homeland Security	71

Appendix VII**GAO Contact and Staff Acknowledgments**75

Tables

Table 1: TWIC Program Funding from Fiscal Years 2002 to 2009	8
Table 2: Three Assessments Planned for TWIC Reader Pilot	11
Table 3: Key TWIC Implementation Actions over Time	59
Table 4: Phased-In Captain of the Port Zone Compliance Schedule (Revised February 19, 2009)	60
Table 5: Scheduling Best Practices	61
Table 6: Assessment of Proposed TWIC Requirements under Consideration in the March 27, 2009, ANPRM for the Card Reader Rule	64

Figures

Figure 1: TWIC Enrollments and Activations over Time	16
Figure 2: TSA Progress in Incorporating Best Practices into Pilot Schedule	28

Abbreviations

ANPRM	Advanced Notice of Proposed Rulemaking
CMMI	Capability Maturity Model Integration
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
ICE	Initial Capability Evaluation
ITT	initial technical testing
MTSA	Maritime Transportation Security Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIN	personal identification number
SAFE Port Act	Security and Accountability For Every Port Act
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

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



United States Government Accountability Office
Washington, DC 20548

November 18, 2009

Congressional Requesters

It is estimated that over 1 million workers, including longshoremen, mechanics, truck drivers, and merchant mariners, access secure areas of the nation's estimated 4,000 maritime-related transportation facilities, such as cargo container and cruise ship terminals, each day while performing their jobs.¹ Securing transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and 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

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program.³ The TWIC program aims to protect the nation's maritime transportation facilities and vessels by requiring maritime workers to complete

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

²GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, [GAO-05-106](#) (Washington, D.C.: Dec. 10, 2004); GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, [GAO-06-982](#) (Washington, D.C.: Sept. 29, 2006); GAO, *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential, but Challenges Remain*, [GAO-07-681T](#) (Washington, D.C.: Apr. 12, 2007); GAO, *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), and GAO, *Transportation Security: Transportation Worker Identification Credential: A Status Update*, [GAO-08-1151T](#) (Washington, D.C.: Sept. 17, 2008).

³DHS's Screening Coordination Office was established in 2006 to coordinate and harmonize the numerous and disparate credentialing and screening initiatives within DHS. With the TWIC program, the Screening Coordination Office facilitates coordination among various DHS components involved in TWIC, such as the Transportation Security Administration and the Coast Guard, as well as the U.S. Citizenship and Immigration Services, which personalizes the credentials, the Federal Emergency Management Agency, which administers the grant funds in support of the TWIC program, and the DHS Science and Technology Directorate, which contributed to the assessment of using TWIC.

background checks and obtain a biometric identification card in order to gain unescorted access to the secure areas of these facilities and vessels.⁴ Key aspects of the program include collecting biographic and biometric information, such as fingerprints, to validate workers' identities; conducting background checks to ensure that workers do not pose a security threat; and issuing tamper-resistant, biometric credentials for use in granting workers unescorted access to secure areas.⁵

TSA's responsibilities include enrolling TWIC applicants, conducting security threat assessments, and processing workers' appeals to adverse TWIC qualification decisions. The Coast Guard is responsible for developing TWIC-related security regulations and ensuring that maritime facilities and vessels are in compliance with these regulations. A federal regulation (known as the credential rule) in January 2007 set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker was required to hold a TWIC in order to obtain unescorted access to secure areas of Maritime Transportation Security Act of 2002 (MTSA) regulated facilities and vessels.⁶ TSA and Coast Guard estimated that approximately 1.2 million workers would use TWICs to access secure areas of maritime vessels and facilities. In August 2008, a pilot was initiated to test the use of TWICs with biometric card readers for granting access to maritime facilities and vessels, and to inform the development of

⁴Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

⁵Biographic information collected includes, for example, a TWIC holder's name and date of birth. According to Coast Guard guidance, a secure area is an area that has security measures in place for access control. For most maritime facilities, the secure area is generally any place inside the outer-most access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. A restricted area is a part of a secure area that needs more limited access and higher security. Under the Maritime Transportation Security Act of 2002 (Pub. L. No. 107-295, 116 Stat. 2064 (2002)) implementing 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.

⁶The credential rule (72 Fed. Reg. 3492 (2007)) established that all maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels were expected to hold TWICs by September 25, 2008, but the final compliance date was extended to April 15, 2009, pursuant to 73 Fed. Reg. 25562 (2008).

the card reader rule (regulation) related to the use of these readers.⁷ In September 2008, we reported that TSA, Coast Guard, and maritime industry stakeholders have faced challenges in implementing the TWIC program, including enrolling and issuing TWICs to a larger population than was originally anticipated, ensuring that TWIC access control technologies perform effectively in the harsh maritime environment, and balancing security requirements with the flow of maritime commerce.⁸

In response to your request, we evaluated TSA and Coast Guard's overall progress in implementing the TWIC program and addressed the following questions: (1) To what extent did TSA, the Coast Guard, and the maritime industry take steps to meet the TWIC compliance date and address related challenges? and (2) What management challenges, if any, do TSA, Coast Guard, and DHS face in executing the TWIC pilot test for informing Congress and the card reader rule?

To identify the steps taken by TSA, the Coast Guard, and the maritime industry to meet the April 15, 2009, TWIC compliance date, and address related challenges, we reviewed program documentation on the status of TWIC enrollment and activation as well as implementation efforts from both TSA and the Coast Guard. Among other things, this documentation includes compliance reports compiled by the Coast Guard from facility-gathered information, TSA's TWIC communication plan for disseminating information about the TWIC enrollment process and compliance deadlines, and program management reviews on TWIC enrollment, activation, and issuance. We analyzed pertinent information including key statutes, such as MTSA, as amended by the Security and Accountability For Every (SAFE) Port Act of 2006,⁹ and related regulations, policies, and

⁷The Federal Emergency Management Agency provided funding for the TWIC pilot participants through federal grants for fiscal years 2006 and 2007. Also, examples of potential requirements being considered as part of the regulation were proposed in an advanced notice of proposed rulemaking issued by the Coast Guard on March 27, 2009, and are listed in appendix V of this report.

⁸GAO-08-1151T.

⁹Pub. L. No. 107-295, 116 Stat. 2064 (2002), as amended by Pub. L. No 109-347, 120 Stat. 1884 (2006).

guidance setting out requirements for the TWIC program.¹⁰ We also reviewed maritime industry documents, such as TWIC Stakeholder Communication Committee meeting minutes and reports by the National Maritime Security Advisory Committee, an advisory council to DHS. We met with nine associations, the members of which are affected by the implementation of TWIC, such as the American Association of Port Authorities—a trade association that represents more than 160 public port organizations—and the Independent Liquid Terminals Association—a trade association representing companies with bulk liquid terminals and above ground storage tank facilities. We also visited four TWIC enrollment and activation centers and visited and met with officials of facilities and vessels affected by TWIC across the country. While information we obtained from these interviews and site visits may not be generalized across the maritime transportation industry as a whole, because the facilities, vessels, and enrollment centers we selected are representative of high and low volume entities in the maritime industry and the enrollment centers are representative of areas with high population density, the locations we visited provided us with an overview of the general progress of the TWIC program, as well as any potential implementation challenges faced by MTSA-regulated facilities/vessels, transportation workers, and mariners. Lastly, we interviewed TWIC program officials from the Coast Guard and TSA—including the TWIC Program Director—regarding their efforts to implement the TWIC program. To assess the extent to which TSA planned for the potential failure of information technology systems supporting the TWIC program in order to minimize the effects of potential TWIC system failures, we reviewed TWIC program management reviews and conducted interviews with TWIC program staff. We compared TSA’s

¹⁰See, for example, Navigation and Vessel Inspection Circular Number 03-07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, DC.: July 2, 2007); Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008); Federal Information Processing Standards (FIPS) Pub 200, *Minimum Security Requirements for Federal Information and Information Systems*, (Gaithersburg, Md., March 2006); National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Gaithersburg, Md.: December 2007); and NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (Washington, D.C.: June 2002).

efforts with internal control standards and industry best practices for contingency planning.¹¹

To identify and assess the management challenges TSA, the Coast Guard, and DHS face in executing the TWIC pilot test for informing Congress and the card reader rule, we reviewed prior GAO reports and testimonies on the TWIC program issued from December 2004 through September 2008, key documents related to the TWIC reader pilot, such as the TWIC Pilot Test and Evaluation Master Plan, the Initial Technical Test Plan, and the Early Operational Assessment Test Plan.¹² We also reviewed relevant legislation, such as the MTSA, as amended by the SAFE Port Act. In addition, we met with various officials at DHS and the Department of Defense to better understand stakeholder contributions and testing approaches related to the TWIC pilot. To further inform our review, we conducted site visits or interviews with officials at each of the seven TWIC pilot sites, and met with local Coast Guard officials and representatives from 15 stakeholder organizations, including associations and business owners from industries impacted by TWIC, such as longshoremens and truck drivers. While information we obtained from the interviews with stakeholders may not be generalized across the maritime transportation industry as a whole, because we selected stakeholders who either represent national associations or who operate in or access the ports where the TWIC reader pilot will be conducted, the interviews provided us with information on the views of individuals and organizations that will be directly impacted by the program. In assessing the TWIC pilot approach,

¹¹See, for example, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, Md., March 2006); NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Gaithersburg, Md.: December 2007); NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (Washington, D.C.: June 2002) and [GAO/AIMD-00-21.3.1](#), *Standards for Internal Control in the Federal Government* (Washington, D.C.: Nov. 1999).

¹²GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, [GAO-05-106](#) (Washington, D.C.: Dec. 10, 2004); GAO, *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, 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), and GAO, *Transportation Security: Transportation Worker Identification Credential: A Status Update*, [GAO-08-1151T](#) (Washington, D.C.: Sept. 17, 2008).

we reviewed the information obtained through these endeavors against best practices we identified in program and project management as well as program evaluation efforts that are relevant to the TWIC program pilot. These practices were identified based on a review of (1) guidance issued by the Office of Management and Budget (OMB);¹³ (2) our prior work on results oriented government, program management and evaluation, and regulatory analysis;¹⁴ and (3) literature on program management principles.¹⁵ We also assessed the pilot schedule against relevant best practices in our Cost Estimating and Assessment Guide to determine the extent to which it reflects key estimating practices that are fundamental to having a reliable schedule.¹⁶ In addition, we compared the TWIC Reader Advanced Notice of Proposed Rulemaking (ANPRM) issued on March 27, 2009, for the card reader rule on using TWICs with biometric card readers to the pilot's test documentation to assess whether the pilot test is considering the proposed characteristics contained in the ANPRM.¹⁷ Appendix I contains more detailed information regarding our scope and methodology.

¹³OMB, Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2007); Circular A-130, *Management of Federal Information Resources* (Nov. 28, 2000); and Circular A-4, *Regulatory Analysis* (Revised Sept. 17, 2003).

¹⁴See for example, GAO, Cost Estimating and Assessment Guide, [GAO-09-3SP](#) (Washington, D.C.: March 2009); GAO, Tax Administration: IRS Needs to Strengthen Its Approach for Evaluating the SRFMI Data-Sharing Pilot Program, [GAO-09-45](#) (Washington, D.C.: Nov. 7, 2008); GAO, Designing Evaluations, [GAO/PEMD-10.1.4](#) (Washington, D.C.: May 1991); and [GAO/AIMD-00-21.3.1](#) Standards for Internal Control in the Federal Government (Washington, D.C.: Nov. 1999); GAO, Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies, [GAO-06-15](#) (Washington, D.C.: October 2005); GAO, Homeland Security: US-VISIT Program Faces Operational, Technological, and Management Challenges, [GAO-07-632T](#) (Washington, D.C. Mar. 20, 2007); and GAO, Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved, [GAO-04-49](#) (Washington, D.C. Jan. 12, 2004).

¹⁵See for example, Project Management Institute's *A Guide to the Project Management Body of Knowledge* (PMBOK Guide), 4th ed. (Newton Square, Pa.: 2008); and Carnegie Mellon's Capability Maturity Model Integration (CMMI®)—CMMI is registered with the U.S. Patent and Trademark Office by Carnegie Mellon University.

¹⁶[GAO-09-3SP](#).

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

We conducted this performance audit from July 2008 through November 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

TWIC Program History

The TWIC program was established in response to several pieces of legislation and subsequent programming decisions. In November 2001, the Aviation and Transportation Security Act (ATSA)¹⁸ was enacted, which included a provision that requires 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. In response to ATSA, TSA established the TWIC program in December 2001.¹⁹ In November 2002, MTSA 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.²⁰ TSA and Coast Guard decided to implement TWIC initially in the maritime domain. In addition, the Security and Accountability For Every (SAFE) Port Act of 2006 amended MTSA to direct the Secretary of Homeland Security to, among other things, implement the TWIC pilot project.²¹ Appendix II summarizes a number of key activities in the implementation of the TWIC program.

In August 2006, DHS officials decided, based on significant industry comment, to implement TWIC through two separate regulations, or rules, the first of which directs the use of the TWIC as an identification

¹⁸Pub. L. No. 107-71, 115 Stat. 597 (2001).

¹⁹TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act enacted on November 25, 2002 (Pub. L. No. 107-296, 116 Stat. 2135 (2002)).

²⁰Pub. L. No. 107-295, 116 Stat. 2064 (2002).

²¹Pub. L. No. 109-347, 120 Stat. 1884 (2006).

credential. The card reader rule, currently under development, is expected to address how the access control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC. On March 27, 2009, the Coast Guard issued an ANPRM for the card reader rule.

From fiscal year 2002 through 2009, the TWIC program had funding authority totaling \$286.9 million. Through fiscal year 2009, \$111.5 million in appropriated funds, including reprogramming and adjustments, has been provided to TWIC (see table 1). An additional \$151.8 million in funding was authorized in fiscal years 2008 and 2009 through the collection of TWIC enrollment fees by TSA, and \$23.6 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. In addition, industry has spent approximately \$179.9 million to purchase 1,358,066 TWICs as of September 24, 2009.²²

Table 1: TWIC Program Funding from Fiscal Years 2002 to 2009

Dollars in millions

Fiscal year	Appropriated	Reprogramming	Adjustments	TWIC fee authority ^a	Federal grant awards related to the TWIC pilot ^b	Total funding authority
2002	0	0	0	0	0	0
2003	\$5.0	0	\$20	0	0	\$25.0
2004	\$49.7	0	0	0	0	\$49.7
2005	\$5.0	0	0	0	0	\$5.0
2006	0	\$15.0	0	0	\$20.9	\$35.9
2007	0	\$4.0	\$4.7	0	\$2.7	\$11.4
2008	\$8.1	0	0	\$42.5	0	\$50.6
2009	0	0	0	\$109.3	0	\$109.3
Total	\$67.8	\$19.0	\$24.7	\$151.8	\$23.6	\$286.9

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

^aFigures in the TWIC fee authority column represent the dollar amount TSA is authorized to collect from TWIC enrollment fees and not the actual dollars collected. For fiscal year 2008, TSA reports to have collected \$41.7 million.

²²Figure based on \$132.50 fee per TWIC.

^bAccording to TWIC program officials, the Port Authority of New York and New Jersey as well as the Staten Island Ferry are using the grant funding received under these programs to support the TWIC pilot as well as other TWIC-related initiatives. Therefore, TWIC officials do not have data on how much of the \$10.5 million provided to these two grant recipients for TWIC-related activities will be used for the TWIC pilot.

Key Components of the TWIC Program's Enrollment, Activation, and Issuance Process

The TWIC program includes several key components:

- **Enrollment:** Transportation workers are enrolled by providing biographic information, such as name, date of birth, and address, and then photographed and fingerprinted at enrollment centers.
- **Background checks:** TSA conducts background checks on each worker to ensure that individuals who enroll do not pose a known security threat. First, TSA conducts a security threat assessment that may include, for example, checks of terrorism databases or watch lists, such as TSA's no-fly list. Second, a Federal Bureau of Investigation criminal history records check is conducted to determine whether the worker has any disqualifying criminal offenses. Third, the worker's immigration status and prior determinations related to mental capacity are checked. Workers are to have the opportunity to appeal negative results of the threat assessment or request a waiver in certain circumstances.
- **TWIC production:** After TSA determines that a worker has passed the background check, the worker's information is provided to a federal card production facility where the TWIC is personalized with the worker's information and sent to the appropriate enrollment center for activation and issuance for each individual applicant.
- **Card activation and issuance:** A worker is informed when his or her TWIC is ready and must return to an enrollment center to select a personal identification number (PIN) and obtain and activate his or her card.²³ Once a TWIC has been activated and issued, the worker may present his or her TWIC to security officials when they seek to enter a secure area, and in the future may use biometric card readers to verify identity.

Once the card is issued, it is presented at MTSA-regulated facilities and vessels in order to obtain access to secured areas of these entities. Current

²³Each TWIC card has a personal identification number (PIN) selected by the TWIC holder at enrollment. This PIN can be used to verify the identity of a TWIC holder against the TWIC. Further, MTSA-regulated facilities and vessels may require TWIC users to use the PIN to unlock biographic information in a TWIC card, such as the TWIC holder's picture.

regulation requires that the card at a minimum be presented for visual inspection.

TSA Is Conducting a Pilot to Test Key TWIC-Related Access Control Technologies

In response to our 2006 recommendation and a SAFE Port Act requirement, TSA initiated a pilot in August 2008²⁴ known as the TWIC reader pilot, to test TWIC-related access control technologies.²⁵ This pilot is intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. As such, the pilot is expected to test the viability of selected biometric card readers for use in reading TWICs within the maritime environment. It is also to test the technical aspects of connecting TWIC readers to access control systems. After the pilot has concluded, the results of the pilot are expected to inform the development of the card reader rule requiring the deployment of TWIC readers for use in controlling access at MTSA-regulated vessels and facilities. Based on the August 2008 pilot initiation date, the card reader rule is 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 4 months prior, or by April 2010.

To conduct the TWIC reader pilot, during the course of our review TSA was partnering with the maritime industry at four ports as well as three vessel operations that are receiving federal grant money for TWIC implementation.²⁶ The participating grantee pilot sites include the ports of Los Angeles, California; Long Beach, California; Brownsville, Texas; and the port authority of New York and New Jersey. In addition, vessel operation participants include the Staten Island Ferry in Staten Island, New York; Magnolia Marine Transports in Vicksburg, Mississippi; and Watermark Cruises in Annapolis, Maryland. Of these seven grant recipients, the four port grant recipients, with input from TSA and Coast Guard, have identified locations at the port where the pilot is to be conducted, such as public berths, facilities, and vessels.

²⁴The pilot initiation date is based on the first date of testing identified in the TWIC pilot schedule. This date is not inclusive of time taken for planning the pilot prior to the first test. The SAFE Port Act required the pilot to commence no later than 180 days after the date of enactment of the SAFE Port Act (October 13, 2006).

²⁵See [GAO-06-982](#).

²⁶As part of DHS's comments on a draft of this report, they noted that the list of pilot participants has changed since the conclusion of this review due to participants withdrawing and the U.S. Coast Guard subsequently adding participants to fill identified gaps.

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 2 below highlights key aspects of the three assessments.

Table 2: Three Assessments Planned for TWIC Reader Pilot

Test name	Description
Initial technical testing (ITT)	This assessment is laboratory based and designed to determine if selected biometric card readers meet TWIC card-reader specifications. ^a These specifications include technical and environmental requirements deemed necessary for use in the harsh maritime environment. At the completion of initial technical testing, a test report is to be developed to prioritize all problems with readers based on their potential to adversely impact the maritime transportation facility or vessel. Based on 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 is 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 include obtaining essential data to inform development of the 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 are 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. To conduct this segment of the pilot, TSA is partnering with maritime transportation facilities at four ports as well as three vessel operators. TSA's objective is 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 is 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 card reader rule. In addition, this evaluation is 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 of 2007 and updated on May 30, 2008.

To address possible time constraints related to using the results of the TWIC pilot to inform the card reader rule, two key changes were made to the pilot test in 2008. First, TSA and Coast Guard inserted a round of testing called the Initial Capability Evaluation (ICE) as the first step of the ITT. The intent of the ICE was to conduct an initial evaluation of readers and determine each reader's ability to read a TWIC. Initiated in August 2008, the ICE testing resulted in a list of biometric card readers from which pilot participants can select a reader for use in the pilot rather than

waiting for the entire ITT to be completed. Further, the ICE list has been used by TSA and Coast Guard to help select a limited number of readers for full functional and environmental testing.²⁷ Second, TSA is no longer requiring the TWIC reader pilot to be conducted in the sequence highlighted in table 2. Pilot sites may conduct early operational assessment and system test and evaluation testing while the initial technical testing is still under way. Currently, ITT testing by TSA is underway and pilot sites are concurrently executing Early Operational Assessment (EOA) testing in varying degrees. Because of the concurrent test approach, some pilot sites may complete ST&E testing while ITT testing remains under way.

²⁷Four readers are to undergo the ITT functional testing and four readers undergo ITT environmental testing, with no reader being required to undergo both functional and environmental testing. ITT full functional testing, or Functional Specification Conformance Test, is to be an evaluation of readers based on their ability to meet the TWIC specifications using thirty-one points of evaluation. As a result of this evaluation, the testing agent is 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, is to include a series of tests to evaluate the card reader's ability to operate in the expected electrical and environmental conditions which exist in the Coastal Ports of the United States of America—such as humidity, salt fog, and dust.

TSA, Coast Guard, and the Maritime Industry Implemented a Number of Measures to Facilitate Enrollment, Activation, and Compliance but Implementation Efforts Were Affected by the Lack of Planning for Potential System Failures

TSA, the Coast Guard, and the maritime industry took several steps to meet the compliance date and address implementation related challenges in an effort to avoid negatively impacting the flow of commerce, but experienced challenges in enrolling transportation workers and activating their TWIC cards. Planning for potential information technology system failures could have helped address one challenge by minimizing the effect of a system failure that affected TSA enrollment and activation efforts. TSA reported enrolling 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million users, as of the April 15, 2009, deadline. Although no major disruptions to port facilities or commerce occurred, TSA data shows that some workers experienced delays in receiving TWICs.

TSA Took Steps to Prepare for a Surge in TWIC Enrollment and Activations, but Experienced Challenges in Meeting the April 2009 Deadline, Including Those Related to Planning for Potential TWIC System Failures

TSA began enrolling maritime workers in the TWIC program in October 2007 through their network of enrollment centers which grew to 149 centers by September 2008. In September 2008 we reported that TSA had taken steps to confront the challenge of enrolling and issuing TWICs in a timely manner to a significantly larger population of workers than was originally anticipated.²⁸ For example, according to TSA officials, the TWIC enrollment systems were tested to ensure that they would work effectively and be able to handle the full capacity of enrollments during implementation. To address issues with the TWIC help desk, such as calls being abandoned and longer-than-expected call wait times, TWIC program management reported that it worked with its contractor to add additional resources at the help desk to meet call volume demand. Similarly, to counter the lack of access or parking at enrollment centers at the Port of Los Angeles, TSA's contractor opened an additional enrollment facility with truck parking access as well as extended operating hours. In addition, TSA reported that it conducted a contingency analysis in coordination

²⁸GAO-08-1151T. The estimate of TWIC enrollees went from the 770,000 workers identified in January 2007 to an estimated 1.2 million—nearly double the original estimate.

with the Coast Guard to better identify the size of its target enrollee population at major ports. For example, in preparation for meeting enrollment demands at the Port of Houston, TWIC program officials updated prior estimates of maritime workers requiring TWICs for access to this port's facilities. Lastly, TSA embarked in a series of communication efforts designed to help inform and educate transportation workers about TWIC requirements and encourage compliance with TWIC. TSA's TWIC communications plan outlines a series of efforts, such as the use of fliers, Web media, and targeted presentations, to inform transportation workers and MTSA-regulated facility/vessel operators. According to TSA officials, the resulting communication efforts contributed to the high number of TWIC enrollments and activations by the April 15, 2009, national compliance date.

Based on lessons learned from its early experiences with enrollment and activation, TSA and its contractor took steps to prepare for a surge in TWIC enrollments and activations as local compliance dates approached.²⁹ For example, as identified in TWIC program documentation and by port facility representatives, TSA and its contractor increased enrollment center resources, such as increasing the number of trusted agents, enrollment stations, and activation stations as needed to meet projected TWIC user demands.³⁰ TSA and its contractor also utilized mobile enrollment centers and employed more flexible hours at enrollment centers in order to accommodate TWIC applicants' needs. For example, at two of the nation's largest ports, the Ports of Los Angeles and Long Beach, TSA and its contractor opened a facility dedicated entirely to TWIC activations in addition to providing additional trusted agents and

²⁹The contractor is responsible for establishing and operating enrollment centers, providing trusted agents to operate enrollment and issuance centers, and providing operations, management and administrative support for the TWIC. While TWIC had a national compliance date of April 15, 2009, TSA and the Coast Guard established a rolling compliance approach, whereby they required affected facilities to comply with TWIC requirements ahead of the national compliance date on a staggered basis by Captain of the Port Zones. A 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. There are 42 such zones in the United States.

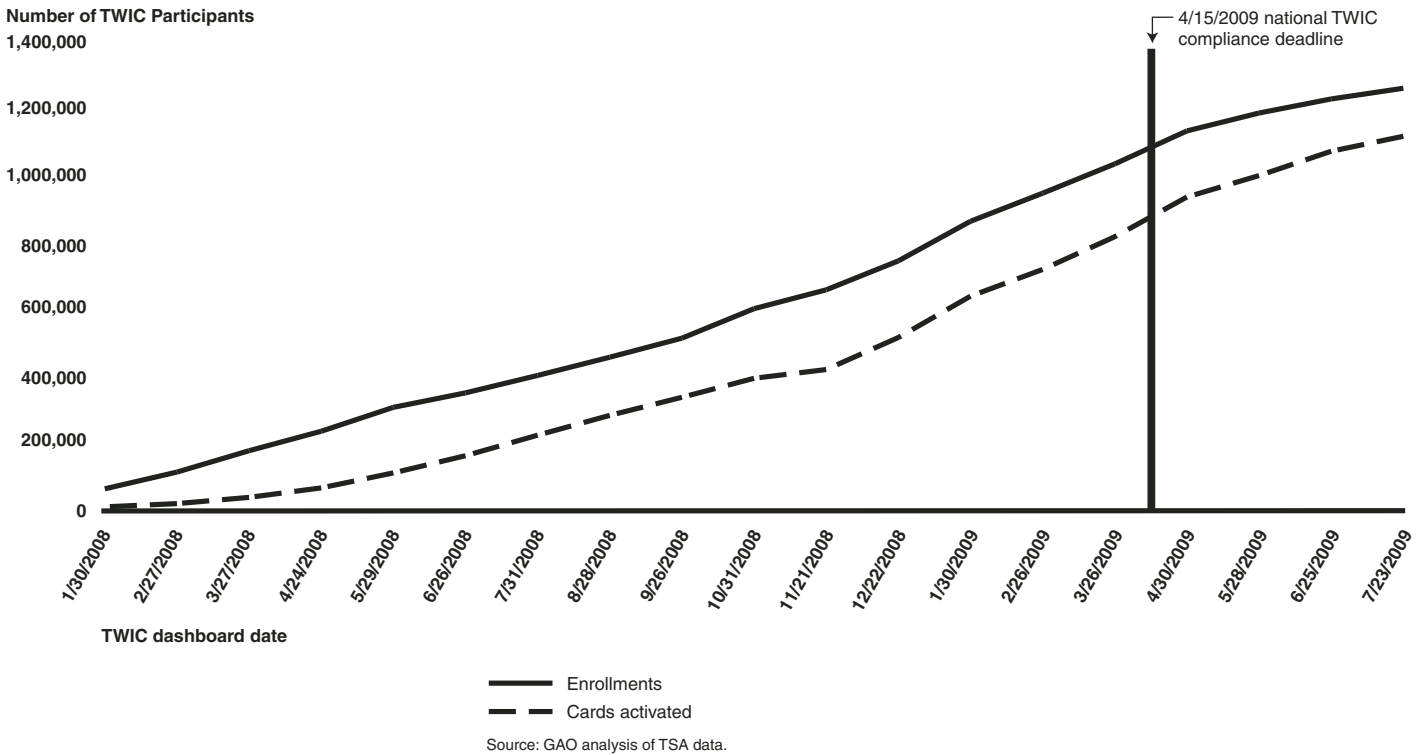
³⁰Trusted Agents (TA) are contractor personnel who possess TWICs and are trained and authorized to collect information and process TWIC enrollments and card activations.

extending hours of operation at enrollment centers.³¹ As a result of these efforts, TSA reported enrolling 1,121,461 workers in the TWIC program, or over 93 percent of the estimated 1.2 million users, by the April 15, 2009, deadline. On this date, the total number of TWIC cards activated and issued reached 906,956, short of the 1,121,461 million enrollees by 214,505 individuals, or 19 percent. According to TSA officials, TWICs were available for 129,090, or approximately 60 percent of these individuals, but had not been picked up by the individual and activated.³² See figure 1 below for details.

³¹The Ports of Los Angeles and Long Beach, ranked first and second out of 124 container ports respectively, have a combined total volume of 74,174,576 metric tons. See USDOT Maritime Administration, *U.S. Waterborne Foreign Container Trade by U.S. Custom Ports* (Updated 04/01/09).

³²According to TSA officials, of the TWIC cards that had not been activated as of April 17, 2009—2 days after the national compliance deadline—129,090 cards were available for activations, but had not been picked up and activated by the TWIC user. Additionally, 7,629 cards were in transit to the enrollment centers; 10,739 cards were in printing or in transit for printing; 10,506 cards were being processed at the Annapolis Junction data center facility; and 47,907 cards were in process with pending data. TSA's figures do not account for the status of 8,634 of the 214,505 enrollments in question.

Figure 1: TWIC Enrollments and Activations over Time



Although no nationwide problem occurred due to TWIC implementation, surges of activity occurred that challenged TWIC enrollment and activation efforts at some locations. For example, at the Port of Baltimore, Coast Guard and port officials stated that, despite multiple communications with TSA about instituting a self-imposed early compliance date, TSA and its contractors were not prepared to handle the increased enrollment demand brought on by the early compliance.³³ As a result, the local fire marshal visited the enrollment center when the number of enrollees exceeded the capacity of the center. In response, TSA

³³In anticipation of the December 1, 2008, TWIC compliance date originally set for the Port of Baltimore, Coast Guard Sector Baltimore, and the Maryland Ports Administration terminals embarked on a coordinated public relations campaign alerting port workers of the upcoming compliance date. When TSA moved the local compliance date back a month to December 30, 2008, the Coast Guard and Maryland Ports Administration officials decided to go forward with the December 1, 2008, date as the date they would begin checking for TWIC cards at the entrance to port facilities.

and its contractor enhanced its enrollment center operations in Baltimore—opening an additional enrollment center at a nearby hotel on the same day—to adapt to the surge in enrollment and activation. In another case, representatives of the New York maritime industry reported that the wait time for employees to receive their TWIC cards following enrollment rose from 6 days to between 6 and 9 weeks as the March 23, 2009, local compliance date approached for Captain of the Port Zone New York. TWIC users in New York also reported difficulty accessing records in the online TWIC database designed as a means for facility operators to verify enrollment in order to grant interim access to employees who had enrolled in the TWIC program but who had not yet received their cards. Furthermore, according to Port of Brownsville and local Coast Guard officials, the lack of resources at the Brownsville enrollment center led to long lines at the center once the local compliance date neared. Additionally, the approach used to notify TWIC applicants that their TWICs were ready for pick-up also proved problematic for Mexican workers. Port of Brownsville officials noted that in many cases these workers have no e-mail and, since many are Mexican citizens, most hold a cell phone with an international phone number (from Mexico). As a result, according to Port of Brownsville officials, many of these enrollees were not adequately notified that their TWIC cards had arrived and were ready for pick-up and activation.

In addition, thousands of TWIC enrollees experienced delays in receiving their TWICs for varying reasons. According to TSA officials and contractor reports, reasons for delayed TWIC issuance included, among others, TSA's inability to locate enrollment records, problems with information on the TWIC cards, such as photo quality, problems with the quality of the manufactured blank cards, and incomplete applicant information required to complete the security threat assessment. Further, TWIC enrollees also experienced delays in obtaining a TWIC because they were initially determined to not be qualified for a TWIC. According to TSA records, as of July 23, 2009, almost 59,000 TWIC applicants received initial disqualification letters and over 30,000 of these applicants appealed the decision questioning the basis for the initial disqualification decision. Under TSA implementing regulations, an applicant may appeal an initial determination of threat assessment if the applicant is asserting that he or she meets the standards for the security threat assessment for which he or she is applying. Almost 25,000 (approximately 42 percent of those receiving initial disqualification letters) of the appeals resulted in an approval upon subsequent review, which suggests that some of these delays could have been avoided if additional or corrected data had been available and reviewed during the original application process. In addition,

about 2,300 of the over 4,800 applicants who requested waivers from the TWIC disqualifying factors were granted them upon subsequent review.³⁴

Advocacy groups, such as the National Employment Law Project (Law Project), have reported that hundreds of individuals experienced delays in receiving their TWICs and that individuals have been unable to work as a result of processing delays at TSA.³⁵ The Law Project has identified at least 485 transportation workers as of June 2009 who requested assistance from it in requesting appeals or waivers from TSA following an initial determination of disqualifying offenses based on TSA's threat assessment. According to officials at the Law Project, for the TWIC applications on which they provided assistance and approvals were granted, it took an average of 213 days between the applicant's enrollment date and final approval for a TWIC. Furthermore, Law Project officials noted that applicants they assisted were out of work for an average of 69 days while waiting for TWIC approval after their port passed the TWIC compliance date. However, TSA could not confirm the figures presented by the Law Project officials because TSA does not track this information in the same format. For example, if a person is sent a disqualification letter and does not respond within 60 days, TSA's system does not continue to track the enrollee's file as an open enrollment waiting to be filled. Rather, TSA closes the file and considers the person to not have passed the threat assessment.³⁶ According to agency officials, when an applicant contacts TSA after the 60-day period passes, TSA routinely reopens their case, though not required to do so, and handles the application until its conclusion. These types of cases often take time to resolve. Similarly, for those situations in which enrollees assert that they never received a disqualification letter and include it as part of the wait time accounted for,

³⁴Under TSA implementing regulations, TSA may issue a waiver of specified provisions relating to, for example, certain disqualifying criminal offenses, and grant a TWIC if TSA determines that an applicant does not pose a security threat based on a review of required information.

³⁵National Employment Law Project, "TWIC Program Reform Prior to April 15, 2009 Compliance Date." Letter to the Chairman of the House Homeland Security Committee and Chairwoman of the Subcommittee on Border, Maritime, and Global Counterterrorism. January 28, 2009.

³⁶TSA reports that as of June 16, 2009, a total of 13,148 TWIC enrollees were issued initial disqualification letters but did not respond within the allowable 60-day time frame. As a result, their applications were converted to a final determination of threat assessment and the enrollee was denied a TWIC.

TSA's numbers will differ as well because, according to TSA officials, they have no way to track whether or not enrollees receive these letters.

Finally, a power failure on October 21, 2008, occurred at the TWIC data center at Annapolis Junction, Maryland—a government facility that processes TWIC data. The power outage caused a hardware component failure in the TWIC enrollment and activation system for which no replacement component was on hand. Consequently, data associated with individual TWICs could not be accessed or processed. As a result of this failure, (1) credential activations were halted until late November 2008 and several TWIC compliance dates originally scheduled for October 31, 2008 were postponed;³⁷ and (2) the failure affected TSA's ability to reset the PINs (i.e., provide users with new PINs) on 410,000 TWIC cards issued prior to the power failure.³⁸ Consequently, TSA will have to replace the cards for cardholders who forget their PINs instead of resetting these PINs. TSA does not know the full cost implications of the power failure at the data center because it is unknown how many of the 410,000 TWIC cards will need to be replaced. Moreover, TSA cannot determine how many of the TWIC cards need to be replaced until all uses for PINs are identified at facilities across the country. For example, one use that will affect the number of TWICs TSA will need to replace is dependant on the number of MTSA-regulated facilities and vessel operators that will require the use of PINs to confirm an individual's identity prior to integrating the user's TWIC into the facility's or vessel's access control system. Officials from two ports we met with stated that the PIN reset problem had caused delays in their system enrollment process, as several enrollees could not remember their PINs and needed to request new TWICs. As of August 1, 2009, TSA reported that 1,246 individuals had requested that their TWIC cards be replaced due to TSA's inability to reset the PINs. While TSA addressed the PIN reset issue by replacing TWICs free of charge, we

³⁷The October 21, 2008, power outage resulted in the postponement of several TWIC compliance dates originally scheduled for October 31, 2008, in the Captain of the Port Zones of Buffalo, New York; Duluth, Minnesota; Detroit and Sault Sainte Marie, Michigan; and Lake Michigan.

³⁸MTSA-regulated facilities and vessels may require TWIC users to use the PIN to unlock information in a TWIC card, such as the TWIC holder's picture, to verify the identity of a TWIC holder against the TWIC.

estimate that it could cost the government \$24,920³⁹ to issue new cards to these individuals and cost the industry \$54,375⁴⁰ in lost personal and work productivity because of time related to the pick-up and activation of the new TWICs. If all 410,000⁴¹ affected TWIC cards need to be replaced, it could cost the government and industry up to approximately \$26 million.⁴²

If TSA had planned for a potential TWIC system failure in accordance with federal requirements in contingency planning and internal control standards, it might have averted the system failure that occurred in October 2008.⁴³ Federal guidance includes having an information technology contingency plan, disaster recovery plan, and supporting system(s) in place. The type of system failure that TSA experienced indicates that TSA did not meet federal requirements for minimal

³⁹Calculation based on the TSA reported figure of production costs being approximately \$20 per card: 1,246 cards × \$20 = \$24,920 approximate cost to the government for TWIC reprints. According to TSA officials, the government has not spent any money on TWIC replacement and related costs, such as providing additional service through the TWIC help desk for a TWIC user to request a new TWIC, shipping the replacement cards to enrollment centers, issuance and activation, and using the time of trusted agents to activate the replacement TWICs. This is because to date, the contractor has absorbed the cost of TWIC replacement and TSA has not yet compensated the contractor for these services. According to TSA officials, the contractor has submitted an adjustment request to TSA to recover its costs for replacing the TWICs. However, at this time, the request and amount to be paid by TSA remains to be negotiated and approved.

⁴⁰Calculation based on TWIC card issuance figures reported by TSA and the Coast Guard in the TWIC Rule 1 regulatory impact analysis: the estimate assumes that on average each worker takes 1.5 hours to travel to and from a center to activate a TWIC. At an hourly wage of \$29.09, it would cost \$43.64 per individual to activate a TWIC. For 1,246 cards, it would cost the industry approximately \$54,375 for reprints.

⁴¹TSA officials state that based on current trend analysis data they believe that the number of TWICs to be reissued due to the power outage will be much less than the 410,000 TWICs potentially affected. However, they do not know if the trend and use of PINs will increase once more facilities and vessels begin to use TWIC readers, or once a rule on the use of TWIC with biometric card readers is issued.

⁴²410,000 cards × \$20 = \$8,200,000 (cost to government); 410,000 cards × \$43.64 = \$17,892,400 (cost to industry); \$8,200,000 + \$17,892,400 = \$26,092,400 or approximately \$26 million in total costs to government and industry.

⁴³FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, Maryland, March 2006); NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, (Gaithersburg, Maryland: December 2007); NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (Washington, D.C.: June 2002); [GAO/AIMD-00-21.3.1, Standards for Internal Control in the Federal Government](#) (Washington, D.C.: Nov. 1999). Contingency planning refers to interim measures to recover information technology services following an emergency or system disruption.

protections for federal systems, which include applying minimum security controls with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. For example, TSA did not have an information technology contingency plan or disaster recovery plan in place to address a potential TWIC system failure.⁴⁴ To minimize the effects of losses resulting from system failures, such plans should provide procedures and capabilities for recovering a major application or facilitate the recovery of capabilities at an alternative site. Moreover, TSA did not have the capabilities or supporting systems in place for recovering the computer system that houses the TWIC data. Nor did TSA have an alternate computer system in place to minimize the effects of a TWIC system failure.

The lack of an approved contingency plan has been a longstanding concern as identified by the DHS Office of Inspector General. In July 2006 the DHS Inspector General identified that a systems contingency plan for TWIC had not been approved or tested.⁴⁵ According to TWIC program management officials, they did not previously implement an information technology contingency plan or develop a disaster recovery plan or supporting system(s) because they did not have funds to do so. Currently, TSA has no effort underway for implementing a contingency plan. However, according to TSA senior officials, they intend to initiate the development of a disaster recovery plan at the beginning of fiscal year 2010. No documentation has been provided, however, to illustrate progress in developing a disaster recovery plan. TSA has, however, identified the lack of a system to support disaster recovery as a risk and has plans to develop one by 2012. While preparing to initiate the development of a disaster recovery plan in the next year and a system to support disaster recovery by 2012 is a positive step, until such plans and system(s) are put in place, TWIC systems remain vulnerable to similar disasters.

⁴⁴The purpose of a contingency plan is to provide procedures and capabilities for recovering a major application or general support system. The purpose of a disaster recovery plan is to provide detailed procedures to facilitate recovery of capabilities at an alternate site. These plans generally identify the procedures and systems to be used during recovery efforts.

⁴⁵See Department of Homeland Security Office of Inspector General, Office of Information Technology, *DHS Must Address Significant Security Vulnerabilities Prior To TWIC Implementation (Redacted)*, DHS/OIG-06-47 (Washington, D.C.: July 7, 2006).

Coast Guard Strategies Helped Meet Compliance Dates and Minimize Compliance-Related Issues

Coast Guard employed strategies to help the maritime industry meet the TWIC national compliance date while not disrupting the flow of commerce. The strategies utilized included using rolling compliance dates and a TWIC temporary equivalency. The TWIC temporary equivalency included allowing workers to gain entry to secure areas of MTSA-regulated facilities/vessels for a limited time without a TWIC by showing proof of, for example, TWIC enrollment and evidence that the individual requesting access had passed the security threat assessment. Below are several examples of the Coast Guard's strategies.

- *Rolling Compliance Dates.* To help ensure that all MTSA-regulated facilities were in compliance by April 15, 2009, the Coast Guard required affected facilities to comply with TWIC requirements ahead of the national compliance date on a staggered basis. (See appendix III for the TWIC compliance schedule.) According to officials from Coast Guard, TSA, and DHS, in executing the rolling compliance approach, Coast Guard required ports with a lower population of TWIC users to comply first, expecting to learn from experiences at these ports prior to requiring compliance at ports with larger populations. For example, the first TWIC deadlines were established for ports in Northern New England, Boston, and Southeastern New England, where Coast Guard anticipated a lower population of TWIC users. The largest ports, which TSA believed would present more of a challenge—the Port of New York and New Jersey, and the Ports of Los Angeles and Long Beach—had TWIC program deadlines of March 23 and April 14, 2009, respectively. Together, these three ports represent 46 percent of total U.S. container volume.⁴⁶
- *TWIC Temporary Equivalency.* In accordance with a policy decision, Coast Guard allowed the use of a TWIC temporary equivalency—or documentation other than an actual TWIC—for a limited time, prior to the national compliance date, to allow TWIC applicants who had passed the security threat assessment access to secure areas of MTSA-regulated facilities/vessels.⁴⁷ For example, in Captain of the Port Zone Corpus Christi, the local TWIC compliance enforcement date was

⁴⁶The Port of New York and New Jersey is the third largest container port in the country with a total container volume of 31,308,727 metric tons. The Ports of Los Angeles and Long Beach, which ranked first and second out of 124 ports respectively, have a combined total volume of 74,174,576 metric tons.

⁴⁷In accordance with a policy advisory council decision, an individual without a TWIC, who showed proof of enrollment and successfully passed the TSA TWIC security threat assessment and presented an identification meeting the requirements of 33 C.F.R. § 101.515, was eligible for access to a MTSA-regulated facility.

November 28, 2008. According to a local Coast Guard official, the sector accepted either the TWIC card or proof that the individual met the temporary equivalency criteria even though they had yet to receive an actual TWIC. This approach was in line with the Coast Guard's desire to ease the administrative burden on maritime workers. Similarly, in Captain of the Port Zone New York, the Coast Guard authorized MTSA-regulated facilities to use a temporary equivalency at their discretion for those individuals in the same situation. Individuals meeting the criteria described above were eligible to continue to access MTSA-regulated facilities until April 15, 2009. On April 1, 2009, the Coast Guard published an update to the policy decision allowing individuals who had enrolled in the TWIC program but had not received their TWIC to be eligible for access to facilities in five Captain of the Port Zones through May 2009 if they met the applicable criteria described above, which includes passing the TSA background investigation.⁴⁸ Similarly, due to card issuance challenges and potential activation back-logs for mariners, on May 28, 2009, the Coast Guard published a new policy decision allowing all U.S.-credentialed mariners eligibility for access to specified U.S. vessels and facilities until July 15, 2009, under similar criteria for the temporary equivalency described above.

The Coast Guard and port strategies also helped to enroll workers in the TWIC program by the national compliance date, and helped to minimize compliance related issues through other strategies. For example, during the first 3 days of compliance for Captain of the Port Corpus Christi, from November 28 through 30, 2008, the Coast Guard conducted 25 spot checks at various facilities, during which they inspected 550 workers. Of these, 430 (78 percent) had their TWIC cards and an additional 109 (20 percent) workers were enrolled but had yet to receive their cards.⁴⁹ No trucks or employees were denied access for lack of a TWIC. Similarly, when Captain of the Port Zones Miami, Key West, and St. Petersburg reached their local compliance date on January 12, 2009, the Coast Guard conducted spot checks of 890 workers from January 13 through January 15, 2009. Of the 890 workers, 709 (80 percent) possessed TWIC cards, and an additional

⁴⁸These Captain of the Port Zones were: Guam; Houston-Galveston, Texas; Port Arthur, Texas; Los Angeles-Long Beach, California; and San Juan, Puerto Rico.

⁴⁹The Coast Guard's compliance reports did not account for the remaining 11 individuals.

164 workers, or 18 percent, were enrolled but had not received their cards.⁵⁰

In addition, during compliance inspections in Captain of the Port Zone Miami, five cargo facilities were found to be noncompliant. Of the five, two were brought into compliance immediately upon identification of the compliance issue with no impact to operations, and three were ordered to suspend MTSA-related operations until they complied with the TWIC requirements. As a result of the suspensions, these facilities could not accept any additional MTSA-regulated vessels until conditions required by the Captain of the Port were met. The Coast Guard worked with the three non-compliant facilities and all were cleared to resume MTSA operations within 2 days. According to one port authority official, the small number of workers and trucks turned away from ports and facilities on the various compliance dates may have been attributable to various factors, such as non-TWIC holders not attempting to enter port facilities, the impact of reduced port traffic due to the downturn in the economy, or facilities providing escorts for non-TWIC holders.

Individual Maritime Ports Employed Different Strategies for Meeting TWIC Compliance Deadlines

Maritime ports across the country also implemented different strategies for meeting their respective TWIC compliance date. Strategies included, among others, enacting compliance exercises ahead of the scheduled compliance date to help identify and address any potential implementation issues that would arise, and requiring a TWIC as part of meeting other locally mandated requirements, such as obtaining a local credential that confirms an individual's eligibility to access a port's facilities.

- While the official local compliance date for Captain of the Port Zone Baltimore was December 30, 2008, the Maryland Port Administration announced that a TWIC would be required for unescorted access to all Maryland Port Administration facilities beginning December 1, 2008, to help sensitize workers to the need to obtain a TWIC. As a result, Baltimore officials reported that most potential compliance issues were addressed in advance of the official local compliance date.
- As of January 15, 2009, the Port Authority of New York and New Jersey made the possession of a TWIC a prerequisite for obtaining or renewing a SeaLink Card—a local credential required by the port

⁵⁰The Coast Guard's compliance reports did not account for the remaining 17 individuals.

authority to verify which drivers are eligible to access facilities under the port authority's jurisdiction. According to port authority officials, by the port's March 23, 2009, local compliance date, over 7,000 of the estimated 8,000 truck drivers and International Longshoremen's Association members that conduct ongoing business at the port had met the requirement. As a result, according to port authority officials, New York did not experience an interruption to commerce on the March 23, 2009, local compliance date.

- At the Ports of Los Angeles and Long Beach, a clean truck program required truckers doing business at the port to also obtain a TWIC by October 1, 2008, in order to participate in the program.⁵¹ As a result, the program requirement helped enroll truck drivers—a population of concern for TWIC program officials—well ahead of the national April 15, 2009, compliance date for the two ports.

Challenges in Program Scheduling and Evaluation May Hinder the TWIC Reader Pilot's Usefulness

Although TSA has made significant progress in incorporating best practices into TWIC's schedule for implementing the reader pilot program, weaknesses continue that limit TSA's ability to use the schedule as a management tool to guide the pilot and accurately identify the pilot's completion date. Moreover, developing a sound evaluation approach for collecting information on the pilot's results could strengthen DHS's approach to help ensure the information collected is accurate and representative of deployment conditions.

⁵¹The Clean Trucks Program at the ports of Long Beach and Los Angeles aims to reduce air pollution from trucks at the port by placing special restrictions on the trucks used for transporting shipments on land.

TSA Has Made Progress Incorporating Best Practices into the TWIC Pilot Schedule, but Weaknesses Exist That Limit Its Usefulness as a Management Tool For Guiding the Pilot and Identifying the Pilot's Completion Date

As we have previously reported, the success of any program depends in part on having a reliable schedule that defines, among other things, when work activities will occur, how long they will take, and how they are related to one another.⁵² As such, the schedule is to not only provide a road map for the systematic execution of a program, but also provide the means by which to gauge progress, identify and address potential problems, and promote accountability. Among other things, best practices and related federal guidance call for a program schedule to be program-wide in scope, meaning that it should include the integrated breakdown of the work to be performed by both the government and its contractors over the expected life of the program.⁵³ Moreover, best practices in project management include sharing documents such as the schedule with stakeholders to attain their buy-in and confirm that the schedule captures the agreed upon activities, time estimates, and other scheduling elements needed to meet project objectives.⁵⁴ Best practices also call for the schedule to expressly identify and define the relationships and dependencies among work elements and the constraints affecting the start and completion of work elements. A well-defined schedule also helps to identify the amount of human capital and fiscal resources that are needed to execute a program.

We have identified nine best practices associated with developing and maintaining a reliable schedule.⁵⁵ These practices include

1. capturing all activities—defining in detail the work to be completed, including activities to be performed;
2. sequencing all activities—listing activities in the order in which they are to be carried out;

⁵²See, for example, GAO, *DOD Business Systems Modernization: Key Marine Corps System Acquisition Needs to Be Better Justified, Defined, and Managed*, [GAO-08-822](#) (Washington, D.C.: July 28, 2008); *Information Technology: FBI Following a Number of Key Acquisition Practices on New Case Management System, but Improvements Still Needed*, [GAO-07-912](#) (Washington, D.C.: July 30, 2007).

⁵³See, for example, [GAO-09-3SP](#); and OMB, *Capital Programming Guide V 2.0, Supplement to Office of Management and Budget Circular A-11, Part 7: Planning, Budgeting, and Acquisition of Capital Assets* (Washington, D.C.: June 2006).

⁵⁴See, for example, [GAO-09-3SP](#); Project Management Institute, *A Guide to the Project Management Body of Knowledge*; and Carnegie Mellon's Capability Maturity Model Integration (CMMI®).

⁵⁵[GAO-09-3SP](#).

-
3. assigning resources to all activities—identifying the resources needed to complete the activities;
 4. establishing the duration of all activities—determining how long each activity will take to execute;
 5. integrating all activities horizontally and vertically—achieving aggregated products or outcomes by ensuring that products and outcomes associated with other sequenced activities are arranged in the right order, and dates for supporting tasks and subtasks are aligned;
 6. establishing the critical path for all activities—identifying the path in the schedule with the longest duration through the sequenced list of key activities;
 7. identifying float between activities—using information on the amount of time that a predecessor activity can slip before the delay affects successor activities;⁵⁶
 8. conducting a schedule risk analysis—using statistical techniques to predict the level of confidence in meeting a project’s completion date; and
 9. updating the schedule using logic and durations to determine the dates for all activities—continuously updating the schedule to determine realistic start and completion dates for program activities based on current information.

See appendix IV for a more detailed explanation of each scheduling practice. In a memo from the DHS Under Secretary for Management dated July 10, 2008, DHS endorsed the use of these practices and noted that DHS would be utilizing them as a “best practices” approach.

TSA has made significant progress during the course of our review in incorporating best practices into the schedule for implementing the TWIC pilot program, although weaknesses continue to exist. Specifically, in response to limitations that we identified and shared with TSA’s program office, the program office developed a new TWIC pilot integrated master schedule in March 2009, and updated it in April 2009, and again in May 2009. As figure 2 illustrates, the pilot schedule went from not meeting any of the nine scheduling best practices in September 2008 to fully addressing one of the practices, addressing seven practices to varying degrees, and not addressing one practice. According to TSA program officials, prior to GAO’s first review of the schedule in September 2008, they had not followed best practices in schedule management because they did not

⁵⁶Float is the amount of times an activity can slip before affecting the critical path.

have enough staffing resources to meet these practices. However, program officials had not developed a workforce plan to determine the number of resources needed to carry out the pilot because, according to these officials, they knew that only two TSA employees and no additional contract staff would be available to perform this work.⁵⁷

Figure 2: TSA Progress in Incorporating Best Practices into Pilot Schedule

Best practice	Extent best practices met		
	September 2008	March 2009	April & May 2009
Capturing all activities			
Sequencing all activities			
Assigning resources to all activities			
Establishing the duration of all activities			
Integrating schedule activities horizontally and vertically			
Establishing the critical path for all activities			
Identifying float between activities			
Conducting a schedule risk analysis			
Updating schedule using logic and durations to determine dates			

- The program provided complete evidence that satisfies the entire criterion
- The program provided evidence that satisfies a large portion of the criterion
- The program provided evidence that satisfies about half of the criterion
- The program provided evidence that satisfies a small portion of the criterion
- The program provided no evidence that satisfies any of the criterion

Source: GAO.

The four areas where TSA’s schedule made the most improvement toward addressing the technical aspects of scheduling best practices include (1) sequencing all activities; (2) integrating schedule activities horizontally and vertically; (3) establishing the critical path for all activities; and (4)

⁵⁷The TWIC pilot is currently in the second of three phases, with plans to be completed by October 4, 2010. This date is 5 months beyond the April 2010 date for reporting to Congress on the results of the pilot. Given the stage of the pilot and reporting time frames, it would not be practical for TSA to develop a workforce plan at this time.

identifying float between activities. For example, in sequencing all activities, the activities identified in the schedule were linked to a single end milestone and pilot sites are no longer scheduled to finish submitting pilot test data on a federal holiday, December 25, 2009—Christmas Day. Furthermore, with regard to integrating the schedule horizontally and vertically, activities contained at different levels of the schedule can now be viewed in relation to each other. In addition, the schedule now identifies a critical path, which is useful for determining which activities are critical for meeting the pilot’s completion date. Finally, the float time identified—or amount of time an activity can be delayed before affecting the project finish date—improved, allowing for a better assessment of the time that each activity can slip before the delay affects the project finish date. For example, one activity in the schedule went from having 249 days of float identified to 59.

While TSA has improved its technical application of program scheduling practices on the TWIC reader pilot program, as of May 2009, weaknesses remain that may adversely impact its usefulness as a management tool and presenting clear insight as to the progress in each phase of the pilot assessment. Weaknesses exist in the following areas:

- *Capturing all activities.* The schedule does not accurately reflect all key pilot activities. For the TWIC pilot, there is no centralized, consolidated document, such as a statement of work, that captures all key activities and can be referred to in order to help assure all intended activities are completed and outcomes achieved for each phase of the pilot testing. While TSA officials acknowledge that each pilot site may take different steps in preparing for and executing the pilot, they said that the assumption applied in developing the schedule is that similar steps are being taken at each site even though each pilot has adopted varying approaches. Moreover, contrary to best practices in program management, the schedule has not been shared with and reviewed by key stakeholders at the pilot sites to capture the varying conditions, or pilot related activities, at each site.⁵⁸ Key stakeholders at the pilot sites would, for example, be able to (1) identify areas that did or did not appropriately describe the full scope of their efforts; (2) identify how the activities at their pilot sites would enable or hinder meeting the activities identified by TSA; and (3) validate the activities identified by

⁵⁸See, for example, [GAO-09-3SP](#); Project Management Institute, *A Guide to the Project Management Body of Knowledge*; and Carnegie Mellon’s Capability Maturity Model Integration (CMMI®).

TSA and durations of the activities. For example, the schedule included having each pilot site complete an environmental related review.⁵⁹ To ensure consistency with federal environmental and historic preservation policies and laws, it is FEMA's policy to require, for example, environmental reviews of each pilot participant in order to receive federal grant funding. However, depending on the level of review to be conducted, it may require more or less effort, or activities, from each grant participant and FEMA to complete. However, the pilot schedule does not account for the activities required to meet the FEMA required environmental reviews or consistently capture the amount of time such reviews would take relative to the level of review to be conducted. Without capturing all activities, TSA's schedule will be inaccurate, thus, hindering its usefulness as a management tool for guiding the pilot and measuring progress.

- *Assigning resources to all activities.* The current schedule does not fully identify the resources needed to do the work or their availability. For example, the schedule does not identify the labor, material costs, and other direct costs needed to complete key activities. Instead, resources are assigned to activities at the organization level (e.g., TSA, Vendor). TSA officials stated that they do not have complete information on or control over the required resources because TSA does not "own the resources" since pilot activities are completed by non-DHS participants, and some funding is provided through FEMA's Port Security and Transit Security Grant programs. However, this should not preclude the TWIC program office from gaining an understanding of what the overall resource requirements are for completing the work. Individual stakeholders, such as pilot participants, could in part be the source of this information. Moreover, while TSA expressed concern over their ability to identify resources for

⁵⁹FEMA requires projects funded through federal grants to conduct an evaluation of the likely environmental effects of projects they propose using. According to FEMA officials, all projects funded through FEMA currently require an Environmental Historical Preservation (EHP) review. These reviews take place post-award and must be completed and approved by FEMA. There are generally three categories of review: Category A projects that have little or no potential for causing a historical or environmental impact; Category B projects that have moderate potential for causing a historical or environmental impact; and Category C projects that have great potential for causing a historical or environmental impact. Each category requires a different level of information and associated activities to complete the review. Category A reviews require the least information and related activities to complete and seldom require additional information from grantees. Category B and C reviews require more information from grantees, such as diagrams and engineering information, which require a greater level of effort (e.g., greater number of activities) from grantees and FEMA than a Category A review.

the pilot in the schedule, officials at pilot sites told us that they had trouble planning for the pilot and allocating resources because they did not fully understand what the pilot was to entail, therefore making it difficult to effectively plan for and identify the needed resources.

- *Establishing the duration of all activities.* The pilot schedule includes duration figures (that is, information on how long each activity is expected to take to perform), but they may not be reliable. According to TSA officials, target dates are discussed with participants for some activities, such as when to start a phase of testing. However, since the pilot program implementation schedule, or relevant segments of the schedule, and related updates are not shared with the pilot participants, it is not clear if the durations TSA's program office associated to each activity are realistic or up-to-date. For example, nearly 86 percent (259 of the 302 activities) of the activities identified in the schedule are based on a 7-day calendar that does not account for weekends or holidays. While normal operations at pilot sites may occur on a 7-day schedule, resources for conducting pilot activities such as installing readers and associated infrastructure such as cables and computers or analyzing the results of pilot data may not be available on the weekend. By using a 7-day schedule, the schedule inaccurately represents approximately 28 percent more days per year being available to conduct certain work than is actually available. Best practices in project management include having stakeholders agree with project plans, such as the schedule.⁶⁰ Because the schedule is not shared with the individual pilots, responsible pilot officials have not been afforded the opportunity to comment on the viability of the 7-day schedule given available resources. Therefore, pilot participants may not have the resources, such as employees available to work on weekends, in order to meet pilot goals. As such, if an activity is defined as taking 60 days, or approximately 2 months using a 7-day calendar, the reality may be that participants work a 5-day work week and as a result the activity takes approximately 3 months to complete—1 month longer than scheduled.

TSA program management officials told us that they believe the impact of using a 7-day versus 5-day calendar is minimal since they understand their key milestones and are committed to meeting the dates they established. Moreover, according to TSA officials, while knowledge of

⁶⁰See, for example, Project Management Institute, *A Guide to the Project Management Body of Knowledge*; and Carnegie Mellon's Capability Maturity Model Integration (CMMI®).

when a task would be completed is important to TSA's management of the pilot, the level of effort (e.g., number of hours) required by the grantees or their contractors to complete the work is not. However, not having a full understanding of how long activities will take to complete has already had an adverse impact on the resource allocation at the Port of Brownsville pilot site. Port officials in Brownsville told us that to meet the date for initiating pilot testing, their contractors had to work unplanned hours to install electrical wiring and fiber optic communication cable needed for the TWIC readers to work. The contractor stated that this required overtime pay, a resource expenditure that was not planned. Therefore, although program management officials may have insight into the schedule using the 7-day approach, the cumulative effect of planning multiple activities to be completed on non-workdays increases the risk that activities will not be completed on time with available resources. Since pilot participants are working on a 5-day schedule, there is a greater risk that key program milestones will not be met, thereby perpetuating inaccuracies in the schedule, and reducing its usefulness as a management and communication tool for ensuring that activities are completed as TSA intended.

- *Conducting a schedule risk analysis.* TWIC program officials have not performed a schedule risk analysis for the pilot schedule because they do not believe it to be necessary. For the TWIC pilot, a schedule risk analysis could enable the program to model "what if" scenarios as to when and if locations such as Long Beach will complete their preliminary work and the effects that schedule changes, if any, might have on meeting the pilot reporting goal. A schedule risk analysis could also help facilitate detailed discussions between the TWIC program office at TSA and the individual pilot locations regarding task durations and expected progress. This is especially relevant for the TWIC pilot given that the schedule does not clearly articulate all of the tasks that need to be completed to carry out the pilot, or changes that may result due to the availability of funding. For example, according to TSA officials and one pilot participant, such changes included delays in FEMA's approval of pilot participants' award contracts to allow the grantees to expend grant funds. In any program that lacks a schedule risk analysis, it is not possible to reliably determine a level of confidence for meeting the completion date.
- *Updating the schedule using logic and durations to determine the dates for all key activities.* The pilot schedule is missing several elements needed to reliably use logic and durations to continuously

update the schedule and determine revised dates for all key activities. Implementing this practice is reliant upon other scheduling practices, such as capturing all activities, assigning resources to all activities, and establishing the duration of all activities. However, the TWIC pilot schedule has not yet fully addressed each of these practices. Thus, schedule updates may not result in reliable dates. Moreover, the current schedule includes date anomalies, such as identifying tasks yet to be started as already having started, and includes 18 activities scheduled in the past for which no actual start date has been identified. For example, the schedule indicates that three activities at the Staten Island pilot site have started on a future date yet to occur. These anomalies indicate the presence of questionable logic in the schedule.

Contrary to best practices in program management, as of August, 2009, TSA had not shared the pilot schedule, or at least relevant segments of the schedule, with pilot participants—all key stakeholders whose buy-in—that is commitment and resources—is needed to ensure that pilot goals and time frames are met.⁶¹ Benefits of sharing the schedule with stakeholders include, for example, confirming the activities needed to complete the pilot, associated resources, activity durations, the viability of attaining milestone dates, and potential risks for schedule slippages. Furthermore, the schedule can serve as a valuable communication tool by helping stakeholders in their individual planning efforts. According to TSA officials, they do not see the value in providing the schedule to pilot participants because it contains too much information. Further, TSA officials told us that they have not shared the schedule with pilot participants due to concerns about sensitive information related to when the pilot results will be provided for congressional review. Lastly, TSA is also concerned that the pilot participants will not have the tools, such as Microsoft Project, available to read and understand the schedule. However, sharing the schedule with pilot participants in a format readable by all can be accomplished using tools such as email or by providing participants with a paper copy. Moreover, to overcome sensitivity issues, TSA could provide participants with the segment of the schedule applicable to the pilot participant and separately inform them of their impact on the overall schedule. Furthermore, having pilot participants, as

⁶¹See, for example, [GAO-09-3SP](#); Project Management Institute, *A Guide to the Project Management Body of Knowledge*; and Carnegie Mellon's Capability Maturity Model Integration (CMMI®).

stakeholders, confirm the viability of key dates and duration of activities, and illustrating the impacts that schedule slippages on any one activity can have on meeting pilot goals and reporting deadlines, can enhance collaboration and communication, help participants in their individual planning efforts, and help minimize future schedule slippages. Without doing so, TSA runs the risk of continuing to manage the program based on an unreliable schedule, further delaying the development of the card reader rule and implementation of the TWIC program with biometric card readers. Since September 2008, TSA has revised its schedule for completing the TWIC reader pilot from October 13, 2009, to a year later, October 4, 2010. Consequently, TSA's current schedule indicates that they will not meet the April 2010 deadline for reporting to Congress on the results of the TWIC reader pilot.

DHS Does Not Have a Sound Evaluation Approach to Ensure Information Collected to Inform Congress and the Card Reader Rule Is Complete, Accurate, and Representative of Deployment Conditions

Shortfalls in TWIC pilot planning have presented a challenge for TSA and Coast Guard in ensuring that the pilot is broadly representative of deployment conditions, and will yield the information needed to inform Congress and a card reader rule aimed at defining how TWICs will be used with biometric card readers. This is in part because an evaluation plan that fully identifies the scope of the pilot and the methodology for collecting and analyzing the information resulting from the pilot has not been developed. Agency officials told us that no such evaluation plan was developed because they believe that the existing pilot documentation coupled with subject matter expertise would be sufficient to guide the pilot and no evaluation plan is needed. However, our review of the TWIC pilot highlights weaknesses that could be rectified by the development of an evaluation plan.

In informing the card reader rule, the TWIC reader pilot is to, among other things, test the technology, business processes, and operational impacts required to deploy card readers at secure areas of the marine

transportation system.⁶² Specifically, the testing is to assess how the TWIC performs when used in conjunction with biometric card readers and systems at maritime facilities and vessels, how the technology performs when used as part of the pilot sites' normal business processes, and to help identify the operational impacts of deploying biometric card readers based on these locations. The pilot results are to help identify the actions necessary to ensure maritime facilities and vessels can comply with the TWIC regulation that is currently being drafted known as the card reader rule.⁶³ In informing the card reader rule, the pilot is also expected to provide information needed for developing the regulatory analysis required by the Office of Management and Budget as part of the rulemaking process.⁶⁴ The regulatory analysis is to demonstrate that examinations of the most efficient alternatives were considered and an evaluation of the costs and benefits—or impacts—to be borne by the government, private sector, and population at large as a result of the regulation were considered.

Consistent with best practices in project management⁶⁵ and our guide for designing evaluations,⁶⁶ in November 2008, we reported that pilot programs can more effectively inform future program rollout when an evaluation plan is developed to guide consistent implementation of the

⁶²The TWIC reader pilot, as defined in the SAFE Port Act of 2006, is to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system. The pilot program is to take place at not fewer than five distinct geographic locations and to include vessels and facilities in a variety of environmental settings. Furthermore, DHS is to report on the following results from the TWIC reader pilot: (1) the findings of the pilot program with respect to technical and operational impacts of implementing a transportation security card reader system; (2) any actions that may be necessary to ensure that all vessels and facilities to which this section applies are able to comply with such regulations; and (3) an analysis of the viability of equipment under the extreme weather conditions of the marine environment.

⁶³The regulation requiring the use of a TWIC for accessing MTSA-regulated facilities and vessels was issued on January 25, 2007.

⁶⁴OMB Circular A-4, *Regulatory Analysis* (Revised Sept. 17, 2003).

⁶⁵See, for example, Carnegie Mellon's Capability Maturity Model Integration (CMMI®). CMMI is registered with the U.S. Patent and Trademark Office by Carnegie Mellon University. Specifically, CMMI identifies typical work products of pilots to include evaluation reports and documented lessons learned. Among other practices, CMMI identifies defining criteria for evaluating pilot results as a critical when planning for a pilot.

⁶⁶GAO, *Designing Evaluations*, [GAO/PEMD-10.1.4](#) (Washington, D.C.: May 1991).

pilot and analysis of the results.⁶⁷ At a minimum, a well-developed, sound evaluation plan contains several key elements, including (1) clear objectives, (2) standards for pilot performance, (3) a clearly articulated methodology, and (4) a detailed data analysis plan. Incorporating these elements can help ensure that the implementation of a pilot generates performance information needed to make effective management decisions.

In planning for and designing the TWIC pilot, DHS—including TSA, Coast Guard, and its Science and Technology Directorate—developed a test and evaluation master plan consisting of several documents.⁶⁸ Together, the TWIC pilot documents address key evaluation plan elements to varying degrees. These documents are useful for identifying planned data collection methods. However, addressing several shortfalls in their planning efforts—such as omissions in the planning methodology and the absence of a data analysis plan to help guide information collection efforts—could strengthen the usefulness of the information collected through the pilot. The following discusses the extent to which key elements are addressed in the TWIC pilot program documentation.

Clear objectives. TWIC pilot documentation identified general program objectives, referred to as the program goals. TWIC program objectives include (1) conducting tests of biometric card readers and the credential authentication and validation process to evaluate the reader specification; and (2) testing the technology, business processes, and operational impacts required to deploy TWIC readers on facilities and vessels prior to

⁶⁷GAO-09-45. Specifically, in [GAO-09-45](#) we reported that a sound, well-developed and documented evaluation plan includes, at a minimum: (1) well-defined, clear, and measurable objectives; (2) criteria or standards for determining pilot-program performance; (3) clearly articulated methodology, including sound sampling methods, determination of appropriate sample size for the evaluation design, and a strategy for comparing the pilot results with other efforts; (4) a clear plan that details the type and source of data necessary to evaluate the pilot, methods for data collection, and the timing and frequency of data collection; and (5) a detailed data analysis plan to track the program's performance and evaluate the final results of the project.

⁶⁸Approved in December 2007, this plan stipulated that an integrated test and evaluation program plan would be developed for the TWIC pilot test. However, instead of developing a single test and evaluation plan for the entire pilot, TSA and Coast Guard officials stated that the separate test plans for each of the three phases of the pilot—initial technical testing, early operational assessment, and system test and evaluation—would together make up the integrated test and evaluation program plan. In March 2009, TSA finalized and approved its test plans for the first two phases of the pilot—the initial technical test phase and the early operational assessment phase. TSA has not yet finalized and approved the test plan for the third and final phase of the pilot—system test and evaluation.

issuing a final rule. The objectives, as stated, articulate the key goals for the pilot. Identifying clear objectives for an evaluation can help ensure that the appropriate evaluation data are collected and that performance can be measured against the objectives.

Performance standards. TSA in conjunction with the Coast Guard developed standards for determining performance for the TWIC pilot, but the standards do not fully address important aspects of the pilot assessment, such as those needed to assess the business and operational impacts of using TWIC with biometric card readers. For example, the master plan identifies some operational performance requirements, such as a minimum reliability threshold, that the card reader is to meet. The plan also identifies technical requirements readers are to meet, such as meeting specific biometric standards or, for example, transaction times. However, the performance standards mostly focus on technology and do not fully identify standards for the business and operational circumstances that using TWIC with biometric card readers will demand. Business and operational circumstances include, for example, the experience a worker will have when attempting to access a secure area of a MTSA-regulated facility, additional steps a worker may need to take to successfully enter a facility, or changes to business processes to accommodate the use of TWIC with readers. Neither the master plan nor subsequent test plans identify performance standards for assessing business and operational performance. For example, there is no test for when a user presents a valid but non-functioning TWIC at an access-control point, and assessing the impact of that scenario on the flow of commerce. TSA officials stated that they had not included this test in the pilot but would consider adding it and others we identified as part of their pilot test. In addition, DHS noted that they expect to identify the business and operational impacts that occur during respective phases of the pilot. While identifying and collecting information on activities as they occur during a pilot can enhance the amount of data collected, incorporating criteria that fully address important aspects of the pilot assessment could strengthen DHS's efforts in determining to what extent the piloted methods are effective.

Clearly articulated evaluation methodology. The methodology for evaluating the TWIC pilot is not fully defined and documented, does not account for differences in pilot design, may not be representative of future plans that individual port facilities have for using TWIC, and does not provide for testing some of the known requirements under consideration

for inclusion in the card reader rule. Thus, such weaknesses may adversely impact the sufficiency and reliability of the information collected from the pilot.⁶⁹

- *The unit of analysis for conducting the pilot, pilot site selection criteria, and the sampling methodology are not fully defined and documented.* The unit of analysis—or the level at which the analysis is to be conducted—had not been defined prior to selecting the facilities and vessels to participate in the TWIC pilot. Specifically, while TSA and Coast Guard intended the unit of analysis to be focused on secure areas, they did not determine whether analysis of pilot test results would be conducted at the port level, facility/vessel level, or the access control point level. As we have previously reported, defining the unit of analysis for any evaluation is particularly important because the results from such an effort will vary depending on this.⁷⁰ With regard to the TWIC pilot, the pilot’s assessment could focus on many different units of analysis. For example, the pilot could be designed to assess the results at a more aggregate level, such as accessing a secured area in its entirety, such as an entire port, facility or vessel. Or, the pilot could focus on the use of readers based on a particular function, such as at trucking lanes or at entranceways for boarding a cruise liner. When designing an evaluation, such as a pilot, it is important to define the unit of analysis and how it may be aggregated at an early stage. This increases the likelihood that the information collected is representative of the information needed for evaluation and can be used to project similar experiences elsewhere. Moreover, as we have previously reported, confronting data collection analysis issues during the design stage may lead to a reformulation of the questions to be addressed as part of an evaluation to ones that can be answered within the time and resources available.⁷¹

TSA officials told us that no specific unit of analysis, site selection criteria, or sampling methodology was developed or documented prior to selecting the facilities and vessels to participate in the TWIC pilot. According to TSA officials, they did, however, take the following factors into account when selecting grant recipients to participate in

⁶⁹Reliability refers to the consistency of results when information is measured or tested and includes the concepts of being verifiable or supported.

⁷⁰GAO, *Quantitative Data Analysis: An Introduction*, [GAO/PEMD-10.1.11](#) (Washington, D.C.: June 1992).

⁷¹[GAO/PEMD-10.1.11](#).

the pilot: (1) the TSA Deputy Secretary suggested including the ports of Los Angeles and Long Beach because they are large volume operations; (2) the Port Authority of New York and New Jersey was selected because of weather conditions and the great mix of traffic (e.g., cargo containers, bulk commodities, and passenger vessels); and (3) the Port of Brownsville was considered because it was in the Gulf region of the United States and it represents a smaller port.⁷² While these general factors were used for selecting the grant recipients to participate in the pilot, the selection factors did not take all evaluation factors into account, such as ensuring that certain types of facilities with specified risk rankings would be selected at each port to facilitate the comparison of pilot results between the different locations. According to TSA officials, they did not identify more specific selection criteria based on the unit of analysis to be evaluated because they believed the factors that they did consider would produce the breadth of maritime operations needed to conduct the pilot. Further, they stated that they could meet evaluation needs by subsequently identifying facilities and vessels at the pilot sites by the type of business they represented (i.e., container facility, liquid storage facility).

However, the pilot documentation does not identify if and how the operations of facilities and vessels at one pilot site are to be compared with those at another site or how the pilot or subsequent evaluation approach is to compensate for the additional factors. For example, additional factors that may impact the ability to compare different sites may include the size of the operation or business processes in place. Moreover, according to TSA officials, they now believe that because TSA and Coast Guard had to rely on volunteer MTSA-regulated facilities and vessels to participate in the pilot, they were limited in their ability to ensure the adequacy of the number and type of selected facilities and vessels for the pilot. The pilot documentation, however, does not yet identify perceived shortcomings with the selected pilot participants, methods for compensating for perceived shortcomings, or evaluation methods to be used to ensure data collected at pilot sites

⁷²To select pilot participants, TSA relied on a pool of candidates that submitted applications for federal port security or transit security grants. In the cases of the Port Authority of New York and New Jersey, the Port of Los Angeles, the Port of Long Beach, and the Port of Brownsville, the grant recipient selected is the port entity its self and not specific facilities or vessels operating at the port. Specific MTSA-regulated facilities and vessels to each port were subsequently selected and agreed to participate in the pilot based on TSA, Coast Guard, and DHS input.

will be comparable and will be representative of the experience of implementing TWIC with biometric card readers across the nation. Further, the documentation does not identify the unit of analysis, define how data are to be analyzed, or how the pilot results are to be compared or contrasted between types of locations, facilities/vessels, or functions. The lack of planning documentation makes it difficult to judge the basis for pilot selection, related constraints, or the extent to which corrective actions have been subsequently applied to compensate for the earlier constraints. Given that the existing evaluation plan documentation does not identify the unit of analysis, define how data are to be analyzed, or how the pilot results are to be compared or contrasted between types of locations, facilities/vessels, or functions, there is a risk that the selected pilot sites and test methods will not result in the information needed to understand the impacts of TWIC nationwide.

- *Differences in pilot designs are not accounted for.* The pilot test and evaluation documentation does not identify how differences in individual pilot site designs and resulting variances in the information collected from each pilot site are to be assessed. This has implications for both the technology aspect of the pilot as well as the business and operational aspect. For instance:

While TSA is applying some controls over the technologies tested at individual pilot sites, it has not identified how the pilot is to compensate for the different technologies tested at each site. For example, as part of its initial capability evaluation, TSA tested a select number of readers to ensure they met certain performance parameters. Furthermore, pilot participants were asked to choose readers that passed the initial capability evaluation. While TSA controlled the population of readers pilot participants could select from, it did not control for alterations made to readers at pilot sites to optimize reader performance or differences in the computers, software, or access control systems with which pilot sites are integrating TWIC readers. Thus, it will be difficult for TSA and the Coast Guard to extrapolate how the use of TWIC-related technologies will be expected to impact the maritime environment as a whole without applying compensating strategies to control for variances to some of these variables. For instance, by not controlling for key variables, such as how a particular site integrates readers with its existing access control system, pilot results may show that a delay related to the use of biometric card readers was incurred, but not appropriately identify the root cause of the delay (e.g., the reader itself or the integration approach).

Business and operational processes and pilot approaches are not the same at each pilot site and a methodology for compensating for the differences has not been developed, thereby complicating the assessment of the results. For example, officials at the Port of Los Angeles said they intend to test all access points at the three MTSA-regulated facilities participating in the pilot test. In contrast, the testing approach at the Port Authority of New York and New Jersey currently includes testing one function at different facilities—such as testing a TWIC reader at 2 of 31 truck lanes at one facility and testing a turnstile in a high volume location at a different facility—instead of all access points at each facility. Further, testing at each port will not necessarily coincide with the time of year with the highest volume of cargo or the environmental conditions for which the pilot sites were selected (e.g., New York in the cold winter months, Brownsville, Texas, during the hottest and most humid months). Without a methodology for compensating for these differences, the information collected may not be comparable or captured in a manner that can be aggregated to assess the impact of TWIC reader deployment on maritime commerce across the nation. According to DHS officials, they understand that this and other limitations exist with the pilot. However, they have decided to proceed with the pilot in this manner, collecting whatever information they can instead of all the information that is needed, because of funding issues. These funding issues include not having the resources to test for every situation they would like and not having control over how pilot participants use the dollars available for the pilot. However, pilot planning documentation does not identify the resources needed to conduct testing for the additional situations, the additional situations TSA and DHS would like to test for, or the testing that will not occur because of insufficient resources. Moreover, TSA and FEMA do have some controls in place to ensure participants use some of the grant funds for the pilot. For instance, as part of the grant process, pilot participants submitted investment justifications to FEMA for approval which were reviewed and approved by FEMA. TSA was provided a copy of each justification and both TSA and Coast Guard reviewed the grantees' plans. Furthermore, pilot participants must submit budget and expenditure reports. Given these steps in the grant management process and coordination between FEMA and TSA, DHS could exert some control over how participants use the dollars available for the pilot.

- *Pilot site test designs may not be representative of future plans for using TWIC.* Pilot participants are not necessarily using the technologies and approaches they intend to use in the future when

TWIC readers are implemented at their sites. In accordance with best practices, pilots should be performed in an environment that is characteristic of the environment present in a broadscale deployment.⁷³ However, officials at two of the seven pilot sites told us that the technology and processes expected to be in place during the pilot will 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. For example, officials we spoke with at one pilot site told us that, during the pilot, the site intends to use a hand held reader solution, but plans to install fixed readers requiring an additional investment in technology infrastructure after the pilot is complete. They are taking this approach because they want to participate in the pilot, but do not want to invest heavily in a solution for the pilot that may not work. As a result of this approach, the information collected from this pilot participant will not be representative of the technology, processes, and cost impacts that implementation of TWIC with biometric card readers will have at the location. Moreover, use of the results captured from this pilot site may hinder the reliability of impact projections made based on this information. Officials at a third pilot site told us that they are using the cheapest solution possible for the pilot because they do not believe that the use of TWIC will ultimately be applicable to them. They said that they would, however, select a different approach if they were likely to have to implement the use of TWIC with biometric card readers.

- *The pilot methodology is not analyzing or testing some of the potential requirements under consideration for inclusion in the card reader rule.* On March 27, 2009, the Coast Guard published the Advanced Notice of Proposed Rulemaking (ANPRM) for the card reader rule.⁷⁴ The ANPRM identifies the requirements under consideration, as defined by the Coast Guard, for deploying TWIC readers at MTSA-regulated facilities and vessels that would be potentially included in the card reader rule on using TWICs with

⁷³For example, Carnegie Mellon's Capability Maturity Model Integration (CMMI®) identifies performing pilots in an environment that is characteristic of the environment present in a broadscale deployment as a practice for pilot process and technology improvements. CMMI is registered with the U.S. Patent and Trademark Office by Carnegie Mellon University.

⁷⁴An ANPRM is published in the Federal Register and contains notices to the public of the proposed issuance of rules and regulations. The purpose of this ANPRM was to encourage the discussion of potential TWIC reader requirements prior to the rulemaking process.

biometric card readers. As such, the ANPRM presents some of the technology, business, and operational requirements that are being considered in developing the card reader rule. Moreover, they represent potential costs and benefits—or impacts—to be borne by the government, private sector, and population at large as a result of the regulation being considered. As such, they are representative of the characteristics that should be included in conducting the TWIC pilot to help ensure that maritime facilities and vessels for which the rule will apply can fully comply with the TWIC rule. However, our review of the ANPRM against the pilot documentation found that the pilot does not address or test some requirements under consideration for the card reader rule.⁷⁵

Of the 27 potential requirements contained in the ANPRM that we assessed, 6 (22 percent) were being tested in the pilot, 10 (37 percent) were partially being tested, and 11 (41 percent) were not being tested (see appendix V for more detail). For example, one potential requirement in the ANPRM is that owners and operators of facilities in the highest risk group may require PINs as an additional level of security.⁷⁶ However, the pilot does not test the use of PINs and the associated impacts the use of PINs could have on access control processes, such as increased waiting times for accessing secure areas or shipping delays. Similarly, another potential requirement being considered in the ANPRM but not tested for in the pilot includes requiring that those owners and operators using a separate physical access control system identify how they are protecting personal identity information. However, the pilot does not test for the impacts of added security on systems to prevent the disclosure of personal

⁷⁵GAO selected the 27 potential requirements evaluated based on our review of the TWIC program, review of maritime industry comments on the ANPRM, and conversations with TSA, the Coast Guard, and pilot participants regarding their experiences with TWIC and the likelihood that the requirements would be strongly considered as part of the proposed regulation on using TWICs with biometric card readers. The 27 requirements are representative of the logical groupings presented in the ANPRM for consideration. The 27 requirements, however, do not represent all requirements identified in the ANPRM, such as testing for each facility and vessel type by assigned risk level. Additionally, the requirements could be further summarized. Also, additional requirements could be under consideration by the Coast Guard that were not presented in the ANPRM.

⁷⁶As stated in the ANPRM, the facilities in the highest risk group include the facilities that are subject to 33 C.F.R. part 104, including (1) facilities that handle certain dangerous cargoes in bulk; (2) facilities that receive vessels certified to carry more than 1,000 passengers; and (3) barge fleet facilities that receive barges carrying certain dangerous cargoes in bulk.

identity information. Such impacts could include, for example, a slow down of system speed for processing a TWIC holder and costs associated with ensuring the actual security of the information maintained in a system. Both of these potential requirements, if implemented, could have operational, technical, and cost implications for maritime commerce.

TSA officials told us that they plan to use the results of our analysis to help them identify additional requirements for testing in the pilot. According to Coast Guard officials, they did not assess each requirement under consideration in the ANPRM against the TSA test documents. Instead, they assessed selected requirements identified in the summary table in the ANPRM.⁷⁷ They said that they plan to supplement the information the pilot provides with data from other sources. While supplementing the information collected can be beneficial, designing the pilot to collect the most information possible about those requirements under consideration for the card reader rule could enhance TSA and Coast Guard's understanding of the viability of certain requirements and related limitations.

Detailed data analysis plan. TSA has not developed a detailed data analysis plan to describe how the collected data is to be used to track the program's performance and evaluate the effectiveness of using TWIC with biometric card readers. Moreover, the available plans do not identify the criteria, methodology, unit of analysis, and overall approach to be used in analyzing the pilot data to ensure that the needed information will result from the pilot. As we previously reported, a detailed analysis plan is a key feature of a well-developed, sound evaluation plan as it sets out who will do the analysis and when and how the data is to be analyzed to measure the pilot project's performance.⁷⁸ Because the information from the pilot is to be used to identify the impact of using TWICs with biometric card readers at maritime facilities and inform the card reader rule (including the related regulatory analysis), a detailed data analysis plan could help ensure that the implementation of the pilot generates performance information needed to make effective management decisions. Without such a plan, it will be difficult for TSA and Coast Guard to validate the results from the pilot and ensure the accuracy and use of the information.

⁷⁷The ANPRM contained a table of potential reader requirements summarizing the requirements Coast Guard is considering for each risk group.

⁷⁸See [GAO-09-45](#).

Consequently, the resulting information may not allow others—such as Congress or external parties affected by the regulation—to independently assess the results and make conclusions about the impacts—including costs and benefits—of implementing TWIC with biometric card readers.

Because the pilot may not provide all of the information needed for implementing the card reader rule and supporting regulatory analysis, Coast Guard officials told us that they would be supplementing the data collected from the TWIC pilot after the pilot is completed rather than adjusting the pilot approach to collect the information. According to Coast Guard officials, they plan to supplement TWIC pilot data by using techniques allowable under federal guidance for developing assessments in support of a federal regulation.⁷⁹ We agree that following the federal guidance should help inform the development of the card reader rule. However, TSA and Coast Guard officials have not identified how information collected outside of the pilot is to be used as part of the evaluation methodology. As we have previously reported, defining what data is needed and how the data is to be used and assessed as part of an evaluation plan can help to ensure information needs are met and properly considered.⁸⁰ TSA and Coast Guard could, for example, augment the information collected from the pilot by leveraging information from other ports that are already or are about to begin using TWICs with biometric card readers. Augmenting the pilot with information from other facilities and vessels that have already implemented TWICs with biometric card readers could help TSA and the Coast Guard meet pilot objectives, and help ensure the pilot effectively informs the card reader rule. By identifying the additional information to be collected along with its source, as well as defining the approach for how the information will be used and compared, TSA and Coast Guard can strengthen their efforts to inform the card reader rule.

Conclusions

TSA has made significant progress in enrolling, activating, and issuing TWICs. As of September 2009, over 1.3 million maritime transportation workers have been enrolled and over 1.1 million TWICs have been activated. Consequently, the enrollment and activation phase of the program for meeting the national compliance date of April 15, 2009, has

⁷⁹See, for example, OMB Circular A-4, *Regulatory Analysis* (Revised Sept. 17, 2003); SBA Office of Advocacy, *A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act* (May 2003).

⁸⁰See, for example, [GAO/PEMD-10.1.11](#); [GAO-09-45](#); and [GAO/PEMD-10.1.4](#).

reached completion. However, the data acquired from workers during this phase of the program and in the future needs to be adequately maintained so that the program can continue uninterrupted and the security aspects of the program can be realized. Since the TWIC system has already failed once—disabling TSA’s ability to reset PINs on TWICs and causing delays in the enrollment of workers and the activation of cards—an approved information technology contingency plan, disaster recovery plan, and supporting system(s) for the computers that store TWIC-related data could help ensure the program’s continuity and effectiveness. While the DHS Inspector General identified the lack of an approved contingency plan in 2006, no steps have been taken to develop such a plan. TSA officials stated that they are planning to develop a disaster recovery plan in fiscal year 2010 and disaster recovery system by 2012. However, until a contingency plan for TWIC systems, including a disaster recovery plan and supporting system(s) as needed are put in place, TWIC systems remain vulnerable.

The potential security benefit of the TWIC program will not be fully realized until maritime transportation facilities install biometric card readers and integrate them with the facilities’ access control systems. The pilot test, intended to inform this phase of the program and the regulation on the use of the card readers in the future, has a number of weaknesses that could negatively affect its rigor and timely completion. Specifically, weaknesses in the pilot schedule limit its usefulness as a management tool for executing the pilot, monitoring its progress, and determining the pilot’s completion date. Until the pilot schedule is shared with pilot participants and updated to accurately reflect realistic resource and time constraints, TSA will lack the management information needed to reliably assess progress towards meeting the planned completion date and pre-emptively identifying likely slippages in the completion date.

Shortfalls in TWIC pilot planning reduce the likelihood that the pilot will be broadly representative of deployment conditions and will yield the technology, business process, and operations information needed to fully and accurately inform the card reader rule. While the pilot does incorporate some useful practices, a comprehensive evaluation plan that identifies the unit of analysis, criteria, and the design and methodology to be used in assessing the data would help ensure that the needed information is collected and recorded during the remainder of the pilot to adequately inform the card reader rule. Furthermore, having an evaluation plan for the pilot could help TSA and the Coast Guard determine the limitations of the pilot and identify where additional information is needed to enhance pilot results and inform the rule. With an understanding of the pilot’s limitations, TSA and Coast Guard would be better positioned to

determine how to compensate for those limitations. While the pilot is currently under way, taking corrective actions to improve the information obtained from the pilot at this time rather than waiting until the pilot is complete and then identifying information shortfalls could prove more time and cost effective for TSA and the Coast Guard. One method for enhancing pilot results could be to leverage the experiences at other nonpilot vessels and facilities in implementing TWIC to date. However, without the foundation of such an effort being grounded in a well developed evaluation plan that defines the information to be collected and approach for obtaining and analyzing the information, TSA and Coast Guard may invest in a well intended effort but not realize the expected results.

Recommendations for Executive Action

To minimize the effects of any potential losses resulting from TWIC system failures, and to ensure that adequate processes and capabilities are in place to minimize the effects of TWIC system interruptions, we recommend that the Assistant Secretary for the Transportation Security Administration direct the TWIC program office to take the following action:

- develop an information technology contingency plan for TWIC systems, including the development and implementation of a disaster recovery plan and supporting systems, as required, as soon as possible.

To help ensure that the TWIC pilot schedule can be reliably used to guide the pilot and identify the pilot's completion date, we recommend that the Assistant Secretary for the Transportation Security Administration direct the TWIC program office, in concert with pilot participants to take the following action:

- fully incorporate best practices for program scheduling in the pilot schedule to help ensure that (1) all pilot activities are captured; (2) sufficient resources are assigned to all activities; (3) the duration of all activities are established and agreed upon by all stakeholders; (4) a schedule risk analysis is conducted to determine a level of confidence in meeting the planned completion date and impact of not achieving planned activities within scheduled deadlines; and (5) the schedule is correctly updated on a periodic basis.

To ensure that the information needed to assess the technical, business, and operational impacts of deploying TWIC biometric card readers at MTSA-regulated facilities and vessels is acquired prior to the development of the card reader rule, we recommend that the Assistant Secretary for the

Transportation Security Administration and Commandant of the U.S. Coast Guard direct their respective TWIC program offices to take the following two actions:

- develop an evaluation plan to guide the remainder of the pilot that includes performance standards, a clearly articulated evaluation methodology—including the unit of analysis and criteria—and a data analysis plan.
- identify how they will compensate for areas where the TWIC reader pilot will not provide the necessary information needed to report to Congress and implement the card reader rule. The information to be collected and approach for obtaining and evaluating information obtained through this effort should be documented as part of an evaluation plan. At a minimum, areas for further review include the potential requirements identified in the TWIC Reader Advanced Notice of Proposed Rulemaking but not addressed by the pilot. Sources of information to consider include investigating the possibility of using information resulting from the deployment of TWIC readers at non-pilot port facilities to help inform the development of the card reader rule.

Agency Comments and Our Evaluation

We provided a draft of this report to the Secretary of Homeland Security for review and comment. DHS provided written comments on behalf of the department and the Transportation Security Administration, the United States Coast Guard, and the Federal Emergency Management Agency on November 5, 2009, which are reprinted in appendix VI. In commenting on our report, DHS stated that it concurred with three of the four recommendations and partially concurred with the other one and identified actions planned or under way to implement them. DHS is taking steps to address our first recommendation related to information technology contingency planning for TWIC systems; however, the actions DHS reported TSA and Coast Guard have taken or plan to take do not fully address the intent of the remaining three recommendations.

With regard to our first recommendation, DHS concurred with our recommendation that TSA develop an information technology contingency plan for TWIC systems, including the development and implementation of a disaster recovery plan and supporting systems. DHS reported that TSA has taken actions to improve contingency planning and disaster recovery capabilities for TWIC related systems. According to DHS, such actions include adding TWIC systems enhancements, such as back-up systems (i.e., redundancy system), and plans for a system Continuity of Operations Plan (COOP) site as part of its Office of Transportation Threat Assessment

and Credentialing's infrastructure modernization effort. TSA's actions to develop a contingency plan for TWIC systems, including a disaster recovery plan and supporting systems, should help enhance TSA's ability to recover operations in the future.

DHS concurred in part with our second recommendation, that TSA, in concert with pilot participants, fully incorporate best practices for program scheduling in the pilot schedule. In its response, DHS agreed that a program schedule is a critical management tool for implementation of the TWIC reader pilot, and notes that its implementation of best practices is tailored to specifically meet the requirements relative to the complex and unique constraints of the pilot program. For example, according to DHS, it focuses its outreach and coordination efforts on the completion of key tasks when risks to the critical path are identified. However, while DHS has made progress in developing the schedule from the TSA perspective, it has not developed the schedule in concert with pilot participants, as we are recommending. As DHS notes, the voluntary nature of the pilot has allowed participants to proceed at their own pace, based on their own local priorities and procedures, making it difficult to develop and maintain accurate activity durations for management purposes. However, based on our review of the TWIC reader pilot schedule, DHS has not accounted for each participant's pace, local priorities and procedures. Instead, DHS, through TSA, identified the activities it deemed to be key for completing the pilot without fully understanding what each participant needs to do to accomplish the key tasks and how long it will take to complete those activities given available resources and local processes. Working individually with its pilot participants to account for program complexities should help ensure that the overall TWIC pilot schedule is informed by each participant, and that key elements—such as the critical path—identified in the schedule developed by TSA are more accurate. Moreover, as noted in our report, the TWIC pilot schedule will not contain the level of information needed for DHS to make effective management decisions despite its efforts to improve its application of scheduling practices. Therefore, additional corrective steps by DHS and TSA are needed to help ensure that the program schedule can be used as a management tool to guide the pilot and accurately identify the pilot's completion date.

DHS also concurred with our third and fourth recommendations, that the TWIC program offices at TSA and Coast Guard (1) develop an evaluation plan to guide the remainder of the pilot that includes performance standards, a clearly articulated evaluation methodology—including the unit of analysis and criteria—and a data analysis plan; and (2) identify how

the agencies will compensate for areas where the TWIC reader pilot will not provide the necessary information needed to report to Congress and implement the card reader rule. We recommended that the information to be collected and approach for obtaining this additional information be documented as part of the evaluation plan. Developing an evaluation plan for a pilot is a prospective endeavor to help guide the identification of needed data and data sources and methods for comparing the data and obtaining the information needed. However, it is not clear from DHS's comments whether their proposed actions will fully address these two recommendations. As our report indicates, while TSA developed a test and evaluation master plan for the TWIC pilot, the document did not identify the business and operational data to be collected during the pilot, the performance standards for assessing the data, or the methodology for evaluating the data. To meet the intent of our recommendations, this information would need to be included in the evaluation plan prior to proceeding with the pilot to ensure that the needed data points are planned for and collected during the pilot in order to inform the mandated report to Congress on the results of the pilot. However, DHS's comments do not indicate that it will take these steps to help inform the report to Congress or the rulemaking process for the TWIC reader rule. Instead, in its response, DHS identifies guidance that it plans to use to supplement the data gathered from the pilot. While identifying the guidance is a positive step, the guidance is not a substitute for a well-developed evaluation plan that defines the information to be collected and approach for obtaining and analyzing the pilot information. Furthermore, the guidance cannot compensate for areas where the TWIC pilot does not provide the necessary information. The plan would help DHS ensure that the pilot serves the purpose Congress intended—collecting the data needed to adequately assess the TWIC program during the pilot.

In its comments to our draft report, DHS, on behalf of TSA, also commented on the October 21, 2008, power outage at the facility that hosts TWIC systems. This outage affected TSA's ability to reset the PINs (i.e., provide users with new PINs) on 410,000 TWIC cards issued prior to the power failure. As part of the regulation that is currently being written, MTSA-regulated facilities and vessels may require TWIC users to use the PIN to unlock information on a TWIC card, such as the TWIC holder's picture, to verify the identity of a TWIC holder. Consequently, TSA will have to replace the cards for cardholders who forget their PINs instead of resetting these PINs. In its response, however, TSA questioned whether it would cost the government and industry up to \$26 million to replace the 410,000 TWIC cards potentially affected by the outage. DHS commented that in the 11 months since the incident, only 1,246 cards have needed

replacement and TSA officials believe it highly unlikely that all 410,000 affected transportation workers will need their cards to be replaced. Although DHS reported that the current number of TWICs replaced remains low, as our report indicates and TSA confirmed, TSA officials will not know the full cost implications of the power failure at the data center until TSA and the Coast Guard start using TWIC cards in conjunction with the electronic access control systems during the next phase of the program. In accordance with the current TWIC regulation, the TWIC is only required to be presented for visual inspection prior to gaining access to a regulated site, and that PINs are not required at this time. This may in part explain the low number of TWICs replaced to date. Based on our review of TWIC use at the seven pilot sites we visited, more TWIC holders are likely to need a TWIC card replacement as more of the nation's estimated 4,000 maritime-related transportation facility operators begin using TWICs in conjunction with electronic access control systems—such as TWIC readers.

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

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. We will then send copies of this report to the Secretary of Homeland Security, the Assistant Secretary for the Transportation Security Administration, the Commandant of the United States Coast Guard, and appropriate congressional committees. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov/>.

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



Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Requesters

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

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

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

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

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

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

Appendix I: Objectives, Scope, and Methodology

This review examined the Transportation Security Administration's (TSA) and Coast Guard's overall progress in implementing the Transportation Worker Identification Credential (TWIC) program. We addressed the following questions: (1) To what extent did TSA, the Coast Guard, and the maritime industry take steps to meet the TWIC compliance date and address related challenges? and (2) What management challenges, if any, do TSA, Coast Guard, and the Department of Homeland Security (DHS) face in executing the TWIC pilot test for informing Congress and the card reader rule?

To identify the steps taken by TSA, the Coast Guard, and the maritime industry to meet the April 15, 2009, TWIC compliance date, and address related challenges, we reviewed program documentation on the status of TWIC enrollment and activation as well as implementation efforts from both TSA and the Coast Guard. Among others, this documentation includes compliance reports compiled by the Coast Guard from facility-gathered information, TSA's TWIC communication plan for disseminating information about the TWIC enrollment process and compliance deadlines, and program management reviews on TWIC enrollment, activation, and issuance. We also interviewed U.S. Citizenship and Immigration Services officials regarding their participation in the TWIC card production and personalization process. In addition, we visited and observed the enrollment process with TSA and TSA contractor representatives at four TWIC enrollment and activation centers. Further, we reviewed TWIC user population estimates and discussed their data reliability with TSA and Coast Guard officials as well as efforts taken to update the population estimates and plan for TWIC enrollment and activation activities and resources. We analyzed pertinent information including key statutes such as the Maritime Transportation Security Act of 2002 (MTSA),¹ as amended by the Security and Accountability For Every (SAFE) Port Act of 2006,² and related regulations, policies, and guidance setting out requirements for the TWIC program.³ We also

¹Pub. L. No. 107-295, 116 Stat. 2064 (2002).

²Pub. L. No. 109-347, 120 Stat. 1884 (2006).

³See, for example, Navigation and Vessel Inspection Circular Number 03-07: *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector* (Washington, D.C.: July 2, 2007); Commandant Instruction M16601.01: *Coast Guard Transportation Worker Identification Credential Verification and Enforcement Guide* (Washington, D.C.: Oct. 10, 2008).

- obtained information from maritime industry stakeholders—such as TWIC Stakeholder Communication Committee—a 15-member advisory council to TSA, Coast Guard, and their contractor to promote real-time communications flow between industry, government, and the TWIC contracting team;
- reviewed reports by the National Maritime Security Advisory Committee—an advisory council to DHS;
- met with nine associations whose members are impacted by the implementation of TWIC, such as the
 - American Association of Port Authorities—a trade association that represents more than 160 public port organizations throughout the Western Hemisphere;
 - The Independent Liquid Terminals Association—a trade association representing companies with bulk liquid terminals and above ground storage tank facilities (“tank farms”) that interconnect with and provide services to various modes of bulk liquid carriers, such as oceangoing tank ships, tank barges, tank trucks, tank rail cars, and pipelines; and
 - The Association of American Railroads—whose members represent a 140,000-mile rail network, including the major freight railroads in the United States, Canada, and Mexico, as well as Amtrak.

We also visited four TWIC enrollment and activation centers, and visited and/or met with officials of facilities and vessels impacted by TWIC across the country such as the ports of Los Angeles and Long Beach, California; Brownsville, Texas; Baltimore, Maryland; and Houston, Texas; as well as the Port Authority of New York and New Jersey. In addition, we met with officials representing vessel operations at the Staten Island Ferry in Staten Island, New York; Magnolia Marine Transports in Vicksburg, Mississippi; Watermark Cruises in Annapolis, Maryland; and World Cruise Terminal in San Pedro, California. At each location, we interviewed officials of facilities and vessels responsible for implementing the use of TWIC. While information we obtained from these interviews and site visits may not be generalized across the maritime transportation industry as a whole, because the facilities, vessels, and enrollment centers we selected are representative of high and low volume entities in the maritime industry and the enrollment centers are representative of areas with high population density, the locations we visited provided us with an overview of the general progress of the TWIC program, as well as any potential implementation challenges faced by MTSA-regulated facilities/vessels, transportation workers, and mariners. Further, we interviewed TWIC program officials from TSA and the Coast Guard—including the TWIC Program Director at TSA and the Coast Guard Commander responsible for the TWIC compliance program—regarding their efforts to implement the

TWIC program. We also interviewed a number of Coast Guard officials at ports across the country regarding local TWIC implementation and compliance efforts to better understand the processes and procedures in place for enforcing compliance with TWIC. Specifically, we interviewed Coast Guard officials with responsibilities in New York and New Jersey; Los Angeles and Long Beach, California; Corpus Christi, Texas; and Baltimore, Maryland. We met with these Coast Guard officials because the facilities, vessels, and enrollment centers we visited are housed in these officials' area(s) of responsibility. To assess the extent to which TSA planned for the potential failure of information technology systems supporting the TWIC program in order to minimize the effects of potential TWIC system failures, we reviewed TWIC program management reviews and conducted interviews with TWIC program staff. We compared TSA's efforts with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance, government internal control standards.⁴

To identify and assess the management challenges TSA, the Coast Guard, and DHS face in executing the TWIC pilot test for informing Congress and the card reader rule, we reviewed prior GAO reports and testimonies on the TWIC program issued from December 2004 through September 2008, and key documents related to the TWIC reader pilot.⁵ These documents included the Broad Agency Announcement-Initial Capability Evaluation, TWIC Pilot Test and Evaluation Master Plan, the Initial Technical Test Plan, the Early Operational Assessment Test Plan, the Concept of

⁴See, for example, FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, Md., March 2006); NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (Gaithersburg, Md.: December 2007); NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* (Washington, D.C.: June 2002) and [GAO/AIMD-00-21.3.1](#), *Standards for Internal Control in the Federal Government* (Washington, D.C.: Nov. 1999).

⁵GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, [GAO-05-106](#) (Washington, D.C.: Dec. 10, 2004); GAO, *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, [GAO-06-982](#) (Washington, D.C.: Sept. 29, 2006); GAO, *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential, but Challenges Remain*, [GAO-07-681T](#) (Washington, D.C.: Apr. 12, 2007); GAO, *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), and GAO, *Transportation Security: Transportation Worker Identification Credential: A Status Update*, [GAO-08-1151T](#) (Washington, D.C.: Sept. 17, 2008).

Operations Plan, TWIC pilot scenarios, the TSA Pilot Schedule, and the Advanced Notice of Proposal Rulemaking on TWIC Reader Requirements. We also collected and analyzed Port Security Grant Program and the Transit Security Grant Program awards relative to the TWIC pilot participants to inform our understanding of the TWIC pilot funding structure and guidance provided to TWIC pilot participants. In addition, we reviewed relevant legislation, such as the MTSA and amendments to MTSA made by the SAFE Port Act of 2006 to inform our review of requirements for TWIC and the TWIC pilot specifically. We also obtained an in person understanding of the benefits of and barriers to implementing the pilot by conducting site visits to or interviews with officials at the 7 pilot sites. Specifically, we visited pilot participants at the Ports of Los Angeles, Long Beach, and Brownsville, and the Port Authority of New York and New Jersey. We also interviewed and or met with officials at vessel operations participating in the TWIC pilot, including the Staten Island Ferry in Staten Island, New York; Magnolia Marine Transports in Vicksburg, Mississippi; and Watermark Cruises in Annapolis, Maryland. To assess the viability of the TWIC pilot and better understand stakeholder contributions within DHS, we met with officials from several components at DHS. Specifically, we met with officials at DHS's Office of Screening Coordination, Science and Technology Directorate, the Coast Guard, the Federal Emergency Management Agency, and the Transportation Security Agency. To further enhance our understanding of the TWIC pilot approach, we also interviewed officials at NIST and the Department of Defense's Naval Air Systems Command and Space and Naval Warfare Systems Command—organizations supporting TSA in the TWIC pilot—to discuss TWIC pilot testing approaches. We also observed testing of TWIC readers against environmental conditions at the Naval Warfare laboratory. In addition, we met with local Coast Guard officials and representatives from 15 stakeholder organizations, including associations and business owners from industries impacted by TWIC, such as longshoremen and truck drivers. While information we obtained from the interviews with stakeholders may not be generalized across the maritime transportation industry as a whole, because we selected stakeholders who either represent national associations or who operate in or access the ports where the TWIC reader pilot will be conducted, the interviews provided us with information on the views of individuals and organizations that will be directly impacted by the program.

In assessing the TWIC pilot approach, we reviewed the information obtained through these endeavors against practices we identified in program and project management as well as program evaluation efforts that are relevant to the TWIC program pilot. These practices were

identified based on a review of (1) guidance issued by OMB;⁶ (2) our prior work on results oriented government, program management and evaluation, and regulatory analysis;⁷ and (3) literature on program management principles.⁸ Based on these recognized standards, practices, and guidance, we

- Assessed the pilot schedule against nine relevant best practices in our Cost Estimating and Assessment Guide to determine the extent to which the pilot schedule reflects key estimating practices that are fundamental to having and maintaining a reliable schedule. In doing so, we independently assessed the program’s integrated master schedule and its underlying activities against our nine best practices. We also interviewed cognizant program officials to discuss their use of best practices in creating the program’s current schedule and we attended three walk-throughs to better understand how the schedule was constructed and maintained. To further assess the reliability of the schedule, we compared information in the pilot schedule to information provided by pilot participants and stakeholders.
- Reviewed TWIC pilot documentation against identified characteristics that sound evaluation plans and approaches include. We also assessed the data to be collected from the TWIC pilot and identified methodologies for using the data to inform Congress on the impacts of using TWIC with biometric card readers and further informing the card reader rule. To help assess the completeness of the TWIC pilot approach and evaluation methodology, we compared the technology,

⁶OMB, Circular A-11, *Preparation, Submission, and Execution of the Budget* (July 2007); Circular A-130, *Management of Federal Information Resources* (Nov. 28, 2000); and Circular A-4, *Regulatory Analysis*, (Revised Sept. 17, 2003).

⁷See for example, GAO, *Cost Estimating and Assessment Guide*, [GAO-09-3SP](#) (Washington, D.C.: March 2009); [GAO-09-45](#), *Tax Administration: IRS Needs to Strengthen Its Approach for Evaluating the SRFMI Data-Sharing Pilot Program*, (Washington, D.C.: Nov. 7, 2008); GAO, *Designing Evaluations*, [GAO/PEMD-10.1.4](#) (Washington, D.C.: May 1991); and [GAO/AIMD-00-21.3.1](#) Standards for Internal Control in the Federal Government (Washington, D.C.: Nov. 1999). GAO, Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies, [GAO-06-15](#) (Washington, D.C.: October 2005); GAO, Homeland Security: US-VISIT Program Faces Operational, Technological, and Management Challenges, [GAO-07-632T](#) (Washington, D.C. Mar. 20, 2007); and GAO, Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved, [GAO-04-49](#) (Washington, D.C. Jan. 12, 2004).

⁸See for example, Project Management Institute’s *A Guide to the Project Management Body of Knowledge* (PMBOK Guide), 4th ed. (Newton Square, Pa.: 2008); and Carnegie Mellon’s Capability Maturity Model Integration (CMMI®)—CMMI is registered with the U.S. Patent and Trademark Office by Carnegie Mellon University.

business, and operational potential requirements identified in the TWIC Reader Advanced Notice of Proposed Rulemaking (ANPRM) issued on March 27, 2009. As part of this assessment we reviewed the program evaluation approach used by TSA and the Coast Guard for leveraging pilot efforts and investments to the maximum extent possible for identifying the cost and other implications on government, the private sector, and the public at large to be considered when developing the regulatory analysis.

We conducted this performance audit from July 2008 through November 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Key TWIC Implementation Actions

Table 3 below summarizes key Transportation Worker Identification Credential (TWIC) program laws and milestones for implementing the program through April 2009.

Table 3: Key TWIC Implementation Actions over Time

Date	Key TWIC implementation actions
November 2002	Enactment of the Maritime Transportation Security Act 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.
August 2004 through June 2005	As part of its prototype testing, TSA—through a private contractor—tested the TWIC program at 28 transportation facilities across the country.
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 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 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.
January 2007	TSA and the Coast Guard issued the credential rule requiring worker enrollment in the TWIC program and TWIC issuance. The Transportation Security Administration also awarded a \$70 million contract to begin enrolling workers and issuing TWICs to workers.
July 2007	The Coast Guard issued guidance on how the maritime industry is to comply with the credential rule and how the Coast Guard will implement TWIC compliance efforts.
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.
October 2008	Phased-In TWIC compliance began at Captain of the Port Zones ^a in Boston, Northern New England, and Southern New England on October 15, 2008.
April 2009	On April 15, 2009, all Captain of the Port Zones nationwide began compliance with TWIC requirements.

Source: GAO summary of TWIC program activities and requirements.

^aA 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.

Appendix III: Phased-In Captain of the Port Zone Compliance Schedule (Revised February 19, 2009)

Table 4 below illustrates the phased-in captain of the port zone compliance schedule from October 2008 to April 2009.

Table 4: Phased-In Captain of the Port Zone Compliance Schedule (Revised February 19, 2009)

October-November 2008	December 2008	January-February 2009	March-April 2009
<u>October 15, 2008</u>	<u>December 1, 2008</u>	<u>January 13, 2009</u>	<u>March 23, 2009</u>
Northern New England Boston	Long Island Sound Charleston	Hampton Roads Morgan City	New York
Southeastern New England	Savannah Jacksonville	New Orleans Upper Mississippi River	<u>April 14, 2009</u> Guam
<u>November 28, 2008</u>		Miami	Houston/Galveston
Corpus Christi	<u>December 1, 2008</u>	Key West	Los Angeles/Long Beach
North Carolina	Buffalo	St. Petersburg	San Juan
Cape Fear River	Duluth Detroit Lake Michigan Sault Ste. Marie		
		<u>February 12, 2009</u>	<u>April 14, 2009</u>
		Honolulu (with the exception of American Samoa)	Port Arthur
	<u>December 30, 2008</u>	South East Alaska	<u>April 14, 2009</u>
	Baltimore	Prince William Sound	American Samoa (within Captain of the Port Zone Honolulu)
	Delaware Bay	Western Alaska	
	Mobile		
	Pittsburgh	<u>February 28, 2009</u>	
	Ohio Valley	Puget Sound	
	Lower Mississippi River	Portland (Oregon)	
	San Diego	San Francisco Bay	

Source: U.S. Coast Guard.

Appendix IV: Scheduling Best Practices

Table 5 presents a summary of best practices identified by GAO for applying a schedule as part of program management.

Table 5: Scheduling Best Practices

Scheduling Best Practices	Explanation
Capturing all activities	The schedule should reflect all key activities as defined in the program's work breakdown structure, which defines in detail the work necessary to accomplish a program's objectives, including activities such as those to be performed by the government and its contractors.
Sequencing all activities	The schedule should be planned so that critical program dates can be met. To meet this objective, key activities need to be logically sequenced—that is, listed in the order in which they are to be carried out. In particular, activities that must be completed before other activities can begin (predecessor activities), as well as activities that cannot begin until other activities are completed (successor activities), should be identified. This helps ensure that interdependencies among activities that collectively lead to the accomplishment of events or milestones can be established and used as a basis for guiding work and measuring progress.
Assigning resources to all activities	The schedule should reflect what resources (e.g., labor, material, and overhead) are needed to do the work, whether all required resources will be available when needed, and whether any funding or time constraints exist.
Establishing the duration of all activities	The schedule should realistically reflect how long each activity will take to execute. In determining the duration of each activity, the same rationale, historical data, and assumptions used for cost estimating should be used. Durations should be as short as possible and have specific start and end dates. The schedule should be continually monitored to determine when forecasted completion dates differ from the planned dates; this information can be used to determine whether schedule variances will affect downstream work.
Integrating schedule activities horizontally and vertically	The schedule should be horizontally integrated, meaning that it should link products and outcomes associated with other sequenced activities. These links are commonly referred to as "hand offs" and serve to verify that activities are arranged in the right order to achieve aggregated products or outcomes. The schedule should also be vertically integrated, meaning that the dates for starting and completing activities in the integrated master schedule should be aligned with the dates for supporting tasks and subtasks. Such mapping or alignment among levels enables different groups to work to the same master schedule.
Establishing the critical path for all activities	Scheduling software should be used to identify the critical path—the path with the longest duration through the sequenced list of key activities. Establishing a program's critical path is necessary to examine the effects of any activity slipping along this path. Potential problems that might occur along or near the critical path should also be identified and reflected in scheduling the duration of high-risk activities.
Identifying float between activities	The schedule should identify the float—the time that a predecessor activity can slip before the delay affects successor activities—so that a schedule's flexibility can be determined. As a general rule, activities along the critical path have the least amount of float time. Total float is the total amount of time by which an activity can be delayed without delaying the project's completion (if everything else goes according to plan).

Appendix IV: Scheduling Best Practices

Scheduling Best Practices	Explanation
Conducting a schedule risk analysis	A schedule risk analysis is performed using statistical techniques to predict the level of confidence in meeting a program's completion date. This analysis focuses on critical path activities and activities near the critical path since they can affect program status. Key aspects of a schedule risk analysis include assessing the level of confidence in meeting a program's completion date, the range of time (i.e., amount of time contingency) needed for a level of confidence, and the identification of high-priority risks. Further, a schedule risk assessment recognizes the interrelationship between schedule and cost and captures the risk that schedule durations and cost estimates may vary due to, among other things: limited data, optimistic estimating, technical challenges, lack of qualified personnel, and other external factors.
Updating the schedule using logic and durations to determine the dates for all key activities	The schedule should be continuously updated using logic and durations to determine realistic start and completion dates for program activities. The schedule should be analyzed continuously for variances to determine when forecasted completion dates differ from planned dates. This analysis is especially important for those variations that impact activities identified as being in a project's critical path and can impact a scheduled completion date. Further, maintaining the integrity of the schedule logic is not only necessary to reflect true status of a project, but is also required before conducting a schedule risk analysis.

Source: GAO.

Appendix V: Assessment of the TWIC Pilot against the Potential TWIC Requirements under Consideration in the March 27, 2009, TWIC Advanced Notice of Proposed Rulemaking for the Card Reader Rule

The analysis below is a detailed review of key statements made in the Transportation Worker Identification Credential (TWIC) Reader Advanced Notice of Proposed Rulemaking (ANPRM) issued by the Coast Guard compared to the items being tested in the TWIC reader pilot. The ANPRM contains the potential TWIC reader requirements Coast Guard is considering as part of a future regulation for MTSA-regulated facilities and vessels required to use TWIC as an access control mechanism. The Coast Guard notes that the ANPRM presents preliminary thoughts on potential requirements for electronic TWIC readers in order to open the public dialogue on implementing TWIC reader requirements. The requirements presented in this ANPRM, represent the technology, business processes, and operational characteristics of TWIC under consideration at the time. Moreover, they represent potential costs and benefits—or impacts—to be borne by the government, private sector, and population at large as a result of the regulation being considered. The TWIC reader pilot, as defined in the SAFE Port Act of 2006, is to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system. Furthermore, The Department of Homeland Security (DHS) is to report on the following results from the TWIC reader pilot: (1) the findings of the pilot program with respect to technical and operational impacts of implementing a transportation security card reader system; (2) any actions that may be necessary to ensure that all vessels and facilities to which this section applies are able to comply with such regulations; and (3) an analysis of the viability of equipment under the extreme weather conditions of the marine environment. The following defines the assessment categories used below.

1. **Yes**—This assessment category represents that the potential requirement identified in the ANPRM is being tested for in the TWIC reader pilot.
2. **Partially**—This assessment category represents that the potential requirement identified in the ANPRM is at least in part being tested for in the TWIC reader pilot.
3. **No**—This assessment category represents that the potential requirement identified in the ANPRM is not being tested for in the TWIC reader pilot.

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

Table 6: Assessment of Proposed TWIC Requirements under Consideration in the March 27, 2009, ANPRM for the Card Reader Rule

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
1. Electronic reader requirements—Integrating TWIC into existing access control systems by using it as a secure means of authenticating an individual when first registering an individual into an existing access control system.	Partially	The TWIC test documentation calls for the collection of data in cases where TWIC is integrated into existing access control systems and using the TWIC to authenticate an individual when first registering the individual for access into a facility. However, the documentation does not set forth a test approach to be used or identify the participants that need to follow the approach in order to ensure the consistency and reliability of the data collected.
2. Electronic reader requirements—Either the contact or contactless ^a interface can be used with existing smart card readers to authenticate the individual and the credential when making access control decisions. (Note: would need to test the requirement for use of each the contact interface and the contactless interface.)	Partially	The TWIC test approach allows for the collection of information on the use of TWIC with biometric card readers that have either a contact or contactless interface. However, the test approach does not identify and compensate for the mix of readers to be used across like facilities in different geographic regions. For example, no mechanism is in place to ensure that similar readers are tested for similar operational environments in each geographic location. Therefore, the information collected may not be comparable.
3. Electronic reader requirements—Use of TWIC physical and logical security features to determine that the TWIC-holder is the same individual to whom the TWIC was issued, and that they do not present a security threat.	Yes	
4. Risk Group A—Applying a different biometric than the fingerprint, such as an iris scan or hand geometry, stored in the local access control system and matched to the individual seeking access. The owner/operator’s system must be linked to the TWIC in such a manner that the access control system forbids access to someone who does not have a valid TWIC, or to someone other than to whom the TWIC has been issued. This means that the TWIC will need to be read and the stored biometric identifier matched against the TWIC-holder’s fingerprint at least once, when the individual is entered into the local access control system.	No	

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
5. Risk Group A—Use of personal identification numbers (PIN) as an additional level of security, during the spot checks, and during annual inspections conducted by the Coast Guard.	No	
6. Risk Group A—Vessels and facilities in the highest risk group (risk group A) authenticate the card electronically with a card reader at each entry. Test the amount of time the transaction between the TWIC-holder and the card reader takes. The readers are to be able to perform this function as the individual is presenting his or her finger for matching against the template stored on the TWIC.	Yes	
7. Risk Group A—Vessels and facilities in risk group A would verify the validity of the TWIC at each entry using information that is no more than 7 days old, when at MARSEC ^b Level 1. ^c This means that on a weekly basis, the Hotlist or Certificate Revocation List (CRL) ^d will need to be downloaded into the reader(s) used at the vessel or facility's access control point(s) or into the local access control system used by the vessel or facility. (Note: would need to test the requirement for each the Hotlist and the CRL.)	Partially	The test documentation references testing for the validity of the TWIC at each entry using Hotlist or CRL information downloaded in varying frequencies, from one day to weekly. However, the documents do not identify if and when testing for each CRL and the Hotlist will be conducted by the pilot site. Therefore, it is not clear if or to what extent, for example, use of the CRL will be tested.
8. Risk Group A—Change in the frequency of Hotlist or CRL download at MARSEC Levels 2 and 3. ^e (Note: would need to test the requirement for each the Hotlist and the CRL).	Partially	The test documentation references testing for the validity of the TWIC at each entry using Hotlist or CRL information downloaded in varying frequencies, from one day to weekly. However, the test documentation does not identify if and when testing for each CRL and the Hotlist will be conducted by pilot site. Further, the pilot testing will not test for changes in processes, such as changing the frequency that the Hotlist or CRL will be downloaded, as would occur during changes in MARSEC levels.
9. Risk Group B—Required to complete the identity verification by using the TWIC as a visual identity badge ("flash pass") at each entry. On a random basis, but at least one day a month, at MARSEC Level 1, they would also be required to match the biometric stored on the card in order to conduct more complete identity verification.	Yes	

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
10. Risk Group B—The validity of the TWICs must be checked at each entry, using TSA’s Hotlist or CRL. (Note: would need to test the requirement for each the Hotlist and the CRL.) At MARSEC Level 1, this would be done using information that is no more than 7 days old. At MARSEC Levels 2 and 3, the information would be downloaded daily.	Partially	The test documentation references testing for the validity of the TWIC at each entry using Hotlist or CRL information downloaded in varying frequencies, from one day to weekly. However, the test documentation does not identify if and when testing for each CRL and Hotlist will be conducted by pilot site. Further, the pilot testing will not test for changes in processes, such as changing the frequency that the Hotlist or CRL will be downloaded, as would occur during changes in MARSEC levels.
11. Risk Group C—Facilities and vessels would not be required to match the biometric stored on the card in order to complete the identity verification at any MARSEC Level. Instead, they would only be required to use the TWIC as a visual identity badge in the manner currently required by the TWIC 1 (credential) federal regulation.	Yes	
12. Risk Group C—Coast Guard has determined that given the type of commodities and small number of passengers typical of this risk group, it is likely these vessels and facilities are a less attractive target for individuals who wish to do harm, though still holding the potential of being involved in a Transportation Security Incident. The card validity check would require only that the expiration date be checked.	Partially	The pilot test addresses this generally by conducting visual inspections. However, testing does not include specifically checking for expiration dates. ^f
13. Risk Group C—The Coast Guard will continue to check and verify TWICs, using handheld readers, during annual inspections and during unannounced spot checks aboard vessels and facilities within all three risk groups.	Yes	
14. Risk Group C—TSA would be able, through use of information collected during enrollment for the TWIC, to contact employers or the Coast Guard if an imminent threat, resulting in an immediate revocation of a TWIC, is identified during the perpetual vetting of TWIC holders.	No ^g	
15. Facilities could be permitted to move between risk groups based on vessel interface or cargo operations.	No	

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
16. Vessels and facilities, at each risk group, using recurring unescorted access for up to 14 persons per vessel or facility. <i>[Further] If recurring unescorted access will be used, test the alternative business and operational processes associated with when and where the initial check of the TWIC will occur, as well as how the periodic card validity check will be accomplished.</i>	No	
17. For recurring unescorted access—Biometric match to include a verification of the Federal Agency Smart Credential-Number (FASC-N) ^h and the TWIC Card authentication Certificate (card authentication), as well as a verification of the validity of the TWIC (card validity check) so long as the validity of the TWIC is verified periodically, using the Hotlist or CRL. ⁱ	Partially	Pilot documentation identifies that testing to assess that a reader can read and verify the attributes identified in the characteristic is generally being conducted. However, testing for this characteristic in conjunction with the business / operational processes associated with an unescorted access provision is not being conducted.
18. For recurring unescorted access, in each case (meaning all risk groups), the validity would need to be checked using information that is no more than 24 hours old.	Partially	Test documents note that all pilot sites will test for TWIC validity. Further, documentation notes that downloading information such as the Hotlist will vary in frequency from daily to weekly. However, the test protocols show that not all test locations, regardless of risk groups, will be using information that is no more that 24 hours old to verify the validity of the TWIC.
19. Owner or operator can pursue an agreement with a facility or other company to borrow or otherwise have access to their reader to perform the initial check, create a file with the FASC-Ns and names of the employees granted recurring unescorted access, and then use a software program to compare the Hotlist or CRL on the required periodic basis. <i>(Note: Relevant testing could, for example, examine the business and operational processes associated with the above characteristic as well as the technology impacts related to the privacy and security of systems used in implementing the approach.)</i>	No	

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
20. Unescorted access process would call for the use of electronic card readers to gain access to certain vessels and the Coast Guard would not require that they be carried on board any vessel... <i>[Further the]</i> recurring unescorted access provisions could be met without requiring installation or implementation of a reader on a gangway or at any other place on the vessel.	Partially	The TWIC reader pilot test does not assess the business processes, operations, or technical aspects of the unescorted access provision. The test methodology does include using readers with TWICs at an offshore location prior to accessing a vessel. However, the testing does not include a review of how this TWIC provision would be carried out in instances where, for example, crew changes or other vessel access can be made from varying locations (i.e., locations other than a vessel's own offshore site). Further, the testing does not consider the impacts of not requiring that vessels carry an electronic card reader on board <i>any</i> vessel, including those instances where a vessel may experience a change in risk level requiring enhanced business processes, operations, and technologies to verify a TWIC.
21. Reader approval based on the standard/specification that will be developed from the results of the TWIC reader pilot program and independent lab.	Yes	
22. <i>For reader calibration and compliance</i> , ensure that once readers are installed, they are maintained in proper working order. Readers would be required to be inspected, tested, calibrated, and maintained in accordance with the manufacturer's recommendations, and that records of those actions be maintained as well. Consideration is being given to whether TWIC readers should also be subject to Coast Guard inspections, or require some type of third-party audit.	Partially	The reader pilot is collecting some information on reader maintenance. However, the test methodology does not test for the operational processes and costs of maintaining repair logs, Coast Guard conducting reader inspections, or conducting a third-party audit.
23. Test for the impact of the business and operational processes put in place on how facility/vessel operators will handle those persons whose TWIC indicate they have poor quality or no fingerprints, as well as those persons that are unable to match their live fingerprint to the template stored on their TWIC.	No	
24. Require that those owners and operators using a separate physical access systems identify how they are protecting personal identity information. <i>(Note: Relevant testing would include obtaining information on, for example, the effects of added security on system speed for processing a TWIC, system costs such as installation and maintenance, and the actual security of the information maintained in a system.)</i>	No	

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

ANPRM potential requirement	Is the potential requirement identified in the ANPRM being tested for in the TWIC reader pilot?	Related information in TWIC reader test documentation
25. The electronic readers should be able to keep track of the names, FASC-Ns, dates, and times of those persons passing through the reader. This may prove beneficial in law enforcement situations.	No	
26. Requiring that facility and vessel owners who are required to utilize readers (those in risk groups A and B) also keep records of the persons who have been granted unescorted access (those whose TWICs have been read by a card reader) for a period of 2 years.	No	
27. Maintain a record to demonstrate that they (meaning the facility/vessel operator) have completed the card validity check (Hotlist or CRL check), if required. <i>(Note: Testing may include, for example, testing of the validity check, the method(s) for maintaining records, and the impacts.)</i>	No	

Source: GAO analysis of U.S. Coast Guard and TSA provided data.

Note: Text in italics above represents additional information provided from GAO analysis to provide additional context for the requirement.

^aReaders for verifying the TWIC can be read either by making contact with a TWIC—that is, inserting the TWIC into a reader—or by introducing the TWIC to the reader by having the TWIC be in close proximity to the reader without having to make physical contact with the reader (e.g., waving a card near a reader).

^bThe Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security’s Homeland Security Advisory System (HSAS). MARSEC levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the U.S. Coast Guard sets MARSEC levels commensurate with the HSAS. MARSEC levels are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

^cMARSEC level 1 means the level for which minimum appropriate security measures shall be maintained at all times. MARSEC 1 generally applies when HSAS threat condition green (representing a low risk of terrorist attack), blue (representing a general risk of terrorist attack), or yellow (representing a significant risk of terrorist attack) are set.

^dBoth the Hotlist and Certificate Revocation List (CRL) are maintained to identify which TWIC cards are valid and which cards are no longer valid.

^eMARSEC level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. MARSEC 2 generally corresponds to HSAS threat condition orange, which represents a high risk of terrorist attack. MARSEC level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target. MARSEC 3 generally corresponds to HSAS threat condition red, which represents a severe risk of terrorist attack.

^fTWIC Rule 1, or the credential rule, on implementing the use of TWIC without readers requires checking the expiration date, the security features on the card, and the photo. However, these checks are not specified in the test documentation. Without this information being specified in the test documents, there is no clear indication of what is being tested.

**Appendix V: Assessment of the TWIC Pilot
against the Potential TWIC Requirements
under Consideration in the March 27, 2009,
TWIC Advanced Notice of Proposed
Rulemaking for the Card Reader Rule**

⁹According to DHS officials, it is DHS policy to ensure revocation of the individual's TWIC and provide proper notification once a threat has been identified. However, DHS has not provided documentation of methods used to ensure that the policy is effectively in place.

¹⁰The FASC-N is an identifying number assigned to each TWIC.

¹¹The documentation does not specify if or how often the Hotlist or CRL will be tested.

Appendix VI: Comments from the Department of Homeland Security

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



**Homeland
Security**

November 5, 2009

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

Dear Mr. Lord:

Thank you for the opportunity to comment on the draft report: "Transportation Worker Identification Credential (TWIC): Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers" (GAO-10-43). The Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning, conducting, and issuing this report.

DHS commends the GAO on recognizing that the program went through national compliance with little to no interruptions and we agree that more work is needed to (1) ensure the execution of the card reader pilot program in a manner that will inform the final rulemaking and (2) facilitate the smooth implementation of reader requirements.

TWIC is a vital security program that is jointly administered by the U.S. Coast Guard (USCG) and the Transportation Security Administration (TSA). TSA is responsible for enrollment, vetting, and card production, while the USCG governs access control requirements and has primary responsibility for enforcement. Additionally, FEMA has administered grants under the Port Security Grant Program (PSGP) for TWIC pilot implementation, and the U.S. Citizenship and Immigration Services (USCIS) provides card production services to TSA.

DHS has made significant progress in implementing the TWIC program, as demonstrated in the successful enrollment of one million workers in less than 18 months and the opening of 150 fixed enrollment centers and 450 mobile sites nationwide. As of October 2009, TSA has enrolled over 1.3 million maritime workers.

DHS has made noteworthy progress on the TWIC reader pilot program. Laboratory testing of readers is largely complete, and TSA has evaluated and published a list of 22 readers to guide pilot test participants in their reader selections. TSA completed extensive testing of five (5) readers in controlled laboratory simulations of the harsh maritime environment and completed functional performance testing of four (4) readers. TSA has begun collecting data during the field test phase of the pilot program, with 24 facility and vessel participants in nine (9) distinct geographic locations representing a significant sampling of Maritime Transportation Security Act (MTSA)-regulated facility and vessel operations. TSA is confident that the data gathered will result in a meaningful final

- 2 -

report to Congress assessing the impacts of deploying TWIC readers as required by the Security and Accountability For Every Port (SAFE) Act of 2006.

As the TWIC program moves forward, DHS will continue to incorporate lessons learned and best practices in order to drive sound management decisions that improve all aspects of the program.

TSA would like to specifically address one comment in GAO's draft report that we believe warrants further clarification. On October 21, 2008, the facility that hosts the TWIC system experienced a power outage. Though power was quickly restored, the part of the system that facilitates card activations and PIN resets was affected. In the report, GAO states that, "if all 410,000 affected TWIC cards need to be replaced, it could cost the government and industry up to approximately \$26 million." TSA notes that it is highly unlikely all 410,000 affected transportation workers will forget their PINs and be unable to remember them within 10 attempts, thus requiring their cards to be replaced. In the 11 months since this incident, only 1,246 cards have needed replacement. Since the October 21, 2008 event, TSA completed a \$1.8 million effort to resolve the system failure vulnerability.

Recommendations for Executive Action

GAO Recommendation [1]: "To minimize the impact of any potential losses resulting from TWIC system failures, and to ensure that adequate processes and capabilities are in place to minimize the impact of TWIC system interruptions, TSA should develop an information technology contingency plan for TWIC systems, including the development and implementation of a disaster recovery plan and supporting systems, as required, as soon as possible."

DHS Concurs: TSA has already taken action to develop and implement an IT contingency and disaster recovery plan for TWIC systems. TSA has reviewed the system architecture to identify single points of failure and has concluded a \$1.8 million effort to implement redundancy and scalability enhancements. This effort resulted in the following improvements:

- Deployment of two additional Card Management CMS servers in the test and production environment using an F5 load balancer configuration
- Deployment of a second Certificate Management Authority in test and production
- Installation of additional AFIS server blades
- Deployment of a second BizTalk server.
- Deployment of a second WebSphere with F5 load balancer
- Deployment of a second IDMS server
- Deployment of a second Oracle database server
- Deployment of a second ISA VPN server

- Deployment of a second HSM server

TSA is in the process of issuing a second task order directed at contingency planning and the further avoidance of system failures. TSA has also included plans for a system COOP site and card production redundancy as part of the Office of Transportation Threat Assessment and Credentialing's Infrastructure Modernization effort.

GAO Recommendation [2]: "To help ensure the TWIC pilot schedule can be readily used to guide the pilot and identify the pilot's completion date, in concert with pilot participants, TSA should fully

- 3 -

incorporate best practices for program scheduling in the pilot schedule to help ensure that (1) all pilot activities are captured; (2) sufficient resources are assigned to all activities; (3) the duration of all activities are established and agreed upon by all stakeholders; (4) a schedule risk analysis is conducted to determine a level of confidence in meeting the planned completion date and impact of not achieving planned activities within scheduled deadlines; and (5) the schedule is correctly updated on a periodic basis.”

DHS Concur in part: DHS agrees that a program schedule is a critical management tool for the implementation of the TWIC reader pilot. The current TWIC reader pilot schedule has implemented best practices and is tailored to specifically meet the management requirements relative to the complex and unique constraints of the pilot program. The voluntary nature of the pilot has allowed each participating port, facility, and vessel operator to proceed at their own pace according to their own local priorities and procedures, making it difficult to develop and maintain accurate activity durations for management purposes.

DHS shared the TWIC pilot schedule with GAO on multiple occasions and incorporated many of GAO’s recommendations during the audit review period. DHS has identified all tasks, estimated durations, and relationships necessary to gather sufficient data and establish a critical path to develop the final pilot report. A common set of tasks has been repeated for all pilot participants when applicable, however the expenditure of grant funds to meet the schedule is reliant on the voluntary participants meeting these tasks and timeframes. DHS uses the schedule as a management tool to assess the overall progress of each participant, focusing outreach and coordination efforts on the completion of key tasks when risks to the critical path are identified through constant monitoring. DHS will continue to update and improve the schedule as new information becomes available during our ongoing, regular dialogue with pilot participants.

GAO Recommendation [3]: “To ensure that information needed to assess the technical, business, and operational impacts of deploying TWIC biometric card readers at MTSA regulated facilities and vessels is acquired prior to the development of the card reader rule, TSA and the U.S. Coast Guard should: (1) develop an evaluation plan to guide the remainder of the pilot that includes performance standards, a clearly articulated evaluation methodology – including the unit of analysis and criteria – and a data analysis plan...”

DHS Concur: DHS continues to mature the evaluation plan to guide implementation of the pilot.

DHS recognizes the importance of thoroughly assessing the technical, business, and operational impacts of deploying TWIC biometric card readers at MTSA regulated facilities and vessels. DHS agrees that documenting the procedures for using pilot data to evaluate these impacts will be worthwhile and timely as we fully expand pilot testing to the field in the coming months. This will allow TSA and the Coast Guard to make any necessary corrections for potential data shortfalls and result in a well-informed rulemaking effort. The Coast Guard and TSA will use OMB Circular A-4, CEQ (NEPA) guidance, and Small Business Administration guidance to inform and develop a baseline data analysis plan to be used for the rulemaking.

GAO Recommendation [4]: “...and identify how they will compensate for areas where the TWIC reader pilot will not provide the necessary information needed to report to Congress and implement the card reader rule. The information to be collected and approach for obtaining and evaluating

- 4 -

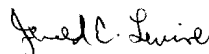
information obtained through this effort should be documented as part of an evaluation plan. At a minimum, areas for further review include the potential requirements identified in the TWIC Reader Advanced Notice of Proposed Rule Making but not addressed by the pilot. Sources of the information to consider include investigating the possibility of using information resulting from the deployment of TWIC readers at non-pilot port facilities to help inform the development of the card reader rule.”

DHS Concurs: DHS intends to augment the data and leverage both the pilot and supplemental data.

In selecting pilot participants, DHS has attempted to ensure that the breadth of MTSA-regulated facilities and vessels are adequately represented. Currently 9 diverse geographic regions are represented in the pilot. Among terminal facilities, there are 8 container operations, 7 bulk cargo operations, 5 petroleum/chemical operations, three passenger terminal operations, 13 operations with significant truck traffic, and four operations with rail traffic. Vessel operations include one 17-vessel towboat operation, two small passenger vessel operations, and one large passenger vessel operation.

TSA will incorporate data gathered from the initial sites volunteering to participate in the test by identifying additional facilities (e.g., APM Virginia Terminals in Portsmouth, Virginia and the Port of Wilmington in Wilmington, Delaware) as either potential full pilot participants, or as contributors who would document their experience introducing TWIC readers apart from the pilot. In cases where an initial pilot participant withdrew from the test TSA has been diligent in finding a suitable replacement if the loss would leave an operation untested. This was the case when Clipper Navigation in Seattle replaced the Catalina Express in Long Beach. Both represent significant high-speed ferry operations, which we believed were critical to the pilot.

Sincerely,



Jerald E. Levine

Director

Departmental GAO/OIG Liaison office

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, David Bruno (Assistant Director), Joseph P. Cruz (analyst-in-charge), Chuck Bausell, Tim Boatwright, Geoffrey Hamilton, Richard Hung, Lemuel Jackson, Daniel Kaneshiro, Stan Kostyla, Jason Lee, Linda Miller, Karen Richey, Julie E. Silvers, and Sally Williamson 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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

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

Public Affairs

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

