United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2006

TRANSPORTATION SECURITY

DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program

GAO-06-982

September 2006

TRANSPORTATION SECURITY

DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-982, a report to congressional requesters

Why GAO Did This Study

The Transportation Security Administration (TSA) is developing the Transportation Worker Identification Credential (TWIC) to ensure that only workers that do not pose a terrorist threat are allowed to enter secure areas of transportation facilities. TSA completed TWIC program testing in June 2005 and is moving forward with implementing the program in the maritime sector by the end of this year. To evaluate the status of the TWIC program, GAO examined (1) what problems, if any, were identified during TWIC program testing and what key challenges, if any, do the Department of Homeland Security (DHS) and industry stakeholders face in implementing the program; and (2) to what extent, if at all, did TSA experience problems in planning for and overseeing the contract to test the TWIC program. To address these issues, GAO interviewed DHS officials and industry stakeholders, reviewed documentation regarding TWIC testing, and conducted site visits to testing locations.

What GAO Recommends

GAO recommends that, before implementing TWIC in the maritime sector, TSA develop and test solutions to problems identified during testing to ensure that key components of the program work effectively and strengthen contract planning and oversight practices before awarding the TWIC implementation contract. DHS reviewed a draft of this report and concurred with GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-982.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

DHS and industry stakeholders face three major challenges in addressing problems identified during TWIC program testing and ensuring that key components of the TWIC program can work effectively in the maritime sector.

- Enrolling workers and issuing TWIC cards in a timely manner to a significantly larger population of workers than was done during testing of the TWIC program.
- Ensuring that the TWIC technology, such as biometric card readers, works effectively in the maritime sector. TSA has obtained limited information on the use of biometric readers in the maritime sector because most facilities that tested the TWIC program did not use these types of readers.
- Balancing the added security components of the TWIC program with the potential impact that the program could have on the flow of maritime commerce.

An independent contractor's assessment found deficiencies with TWIC program testing and recommended that additional testing be conducted to determine its effectiveness. TSA has acknowledged that there are challenges to implementing the TWIC program and has taken some actions to address these issues, including allowing more time to consider requirements for installing TWIC access control technologies. However, TSA plans no additional testing of the TWIC program. Rapidly moving forward with implementation of the TWIC program without developing and testing solutions to identified problems to ensure that they work effectively could lead to further problems, increased costs, and program delays without achieving the program's intended goals.

TSA experienced problems in planning for and overseeing the contract to test the TWIC program. Specifically, TSA made a number of changes to contract requirements after the contract was awarded, contributing to a doubling of contract costs, and TSA did not ensure that all key components of the program were tested. TSA has acknowledged that problems with contractor oversight occurred because the agency did not have sufficient personnel to monitor contractor performance. TSA has taken some actions to address this problem. However, until TSA issues the contract for TWIC implementation and develops its plans for monitoring contractor performance, it is not clear to what extent these actions will ensure that the contract to implement the TWIC program will include comprehensive and clearly defined requirements and that contractor performance will be closely monitored to ensure that the program is implemented successfully and costs are controlled.

Biometric TWIC Card Reader

Source: GAO.

Contents

Figures

Abbreviations

ATSA	Aviation and Transportation Security Act
COTR	contracting officer technical representative
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standard
HSPD	Homeland Security Presidential Directive
MTSA	Maritime Transportation Security Act
OCS	outer continental shelf
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 29, 2006

The Honorable Susan M. Collins
Chairwoman
The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ted Stevens
Chairman
The Honorable Daniel K. Inouye
Co-Chairman
Committee on Commerce, Science, and Transportation
United States Senate

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

Protecting the nation's transportation facilities, including seaports, airports, and railroad terminals, from the threat of terrorism has taken on special urgency in the post–September 11, 2001, environment. These facilities are critical components of the U.S. economy and are necessary for supplying goods throughout the country and supporting international commerce. For example, the Ports of Los Angeles and Long Beach estimate that they alone handle 43 percent of the nation's oceangoing cargo. An attack at one of these port facilities could severely affect the country's economy. About 6 million workers, including longshoreman, mechanics, aviation and railroad employees, truck drivers, and others access secure areas of the nation's estimated 4,000 transportation facilities each day while performing their jobs. Some of these workers, such as truck drivers, regularly access secure areas at multiple transportation facilities. Ensuring that only workers that do not pose a terrorist threat are allowed access to secure areas is important to preventing an attack. In the

aftermath of the September 11, 2001, terrorist attacks, the Aviation and Transportation Security Act (ATSA)[1] was enacted in November 2001 and, among other things, requires the Transportation Security Administration (TSA), an agency within the Department of Homeland Security (DHS), to work with airport operators to strengthen access control points in secure areas and consider using biometric access control systems to verify the identity of individuals who seek to enter a secure airport area. In response to ATSA, TSA established the Transportation Worker Identification Credential (TWIC) program in December 2001 to mitigate the threat of terrorists and other unauthorized persons from accessing secure areas of the entire transportation network.[2] In November 2002, the Maritime Transportation Security Act of 2002 (MTSA)[3] was enacted which, among other things, required the Secretary of DHS to issue a maritime worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels. TSA intends the TWIC program to satisfy the requirements of MTSA and to enhance access control security across all modes of transportation.

The purpose of the TWIC program is to protect the nation's transportation facilities from the threat of terrorism by issuing identification cards only to workers who do not pose a terrorist threat and allow these workers unescorted access to secure areas of our nation's transportation system. To accomplish this objective, the TWIC program is to include background checks on transportation workers to ensure they do not pose a threat to security, collection of personal and biometric information to validate workers' identities, issuance of tamper resistant biometric credentials that cannot be counterfeited, verification of these credentials using biometric access control systems before a worker is granted unescorted access to a secure area, and revocation of credentials if workers are found to pose a threat to security or if a card is lost or stolen.

In December 2004, we reported on the status of the TWIC program. Specifically, we described the reasons TSA cited for continued program delays and recommended that TSA develop plans to better manage the project, identify risks to the program, and analyze the costs and benefits of

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

[2] TSA was transferred from the Department of Transportation to the new Department of Homeland Security pursuant to requirements in the Homeland Security Act of 2002 (Pub. L. No. 107-296, 116 Stat. 2135 (2002).

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

program alternatives.[4] TSA agreed with these recommendations. TSA—through a private contractor—tested the TWIC program from August 2004 to June 2005 at 28 transportation facilities around the nation. In August 2005, the TWIC testing contractor submitted a report summarizing the results of the TWIC testing to TSA.

Recently, the proposal to transfer control of the operations of various U.S. port terminals to a foreign company heightened concerns regarding the security of the nation's transportation system, specifically related to access at ports. In response to these concerns, the Secretary of DHS announced in April 2006 that the TWIC program had been delayed too long and that DHS would accelerate implementation of the program beginning in the maritime sector. In May 2006, DHS issued a proposed rule that describes the requirements of the TWIC program that the owners and operators of maritime facilities and vessels would be required to implement. The maritime industry was provided the opportunity to comment on the proposed rule until July 6, 2006. In August 2006, DHS decided that the TWIC program would be implemented in the maritime sector using two separate rules in response to numerous maritime industry concerns about whether the access control technologies necessary to operate the TWIC program will work effectively. One rule will cover enrolling workers and issuing cards and a second rule will cover implementing TWIC access control technologies, such as biometric card readers. DHS plans to finalize the first TWIC rule by the end of calendar year 2006, and the second TWIC rule will be issued subsequently. TSA estimates that implementation of the TWIC program in the maritime sector will cost the federal government and transportation facilities about $800 million over the next 10 years. TSA estimates that individuals applying to receive a TWIC card will be charged a fee of $149. According to TSA, the agency is considering implementing TWIC in other modes of transportation in the future, but has not established a time frame for doing so.

To help Congress evaluate TSA's overall progress in implementing the TWIC program, we answered the following questions: (1) What problems, if any, did testing of the TWIC program identify and what challenges, if any, do DHS and industry stakeholders face in implementing the program?

[4] GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: December 2004).

and (2) To what extent, if at all, did TSA experience problems in planning for and overseeing the contract to test the TWIC program?

To answer these questions, we interviewed officials from the two DHS components responsible for implementing the TWIC program, TSA and the Coast Guard. Specifically, we interviewed these officials regarding the development and implementation of the TWIC program, the results of tests of the key components of the TWIC program, the challenges of implementing the program, and the planning for and oversight of the contract to test the TWIC program. To determine the goals and requirements of TWIC testing, testing results, and status of the TWIC program, we obtained and analyzed TWIC program documents, including program management plans, the contract for testing the TWIC program, the final report on the test results, an independent assessment of TWIC testing, and the TWIC proposed rule and the corresponding regulatory impact analysis. We also reviewed applicable laws, regulations, policies, and procedures to determine the requirements for implementing the TWIC program. In addition, we interviewed TWIC testing contractor officials concerning testing results, oversight provided by TSA, and the independent assessment of TWIC testing. We also interviewed officials from the contractor that performed an independent assessment of TWIC testing. We also reviewed TSA policies and procedures for contract oversight related to monitoring the performance of contractors. We conducted site visits to 15 of the 28 facilities that participated in testing the TWIC program in California, Delaware, Florida, New Jersey, New York, and Pennsylvania to observe the operation of the TWIC program at these facilities, obtain information on stakeholder experiences related to the TWIC testing, and discuss any challenges associated with implementing TWIC.[5] We visited testing facilities in each of the three testing regions, East Coast, West Coast, and Florida, as well as locations representing three modes of transportation—maritime, aviation, and rail. We attended three of the four public meetings held by TSA and the Coast Guard in May and June 2006 to obtain industry comments on the TWIC proposed rule and reviewed stakeholder comments submitted to TSA and the Coast Guard during the rulemaking process. This work was also informed by our prior reports and testimony related to TWIC, maritime and transportation security, and TSA and DHS contracting practices. More detailed information on our scope and methodology is contained in

[5] We selected the 15 facilities based on geographic location, mode of transportation, diversity of facility size, and area of business operations.

appendix I. We conducted our work from August 2005 through September 2006 in accordance with generally accepted government auditing standards.

Results in Brief

DHS and industry stakeholders face three major challenges in addressing problems identified during TWIC program testing and ensuring that key components of the TWIC program can function effectively. The first challenge is enrolling and issuing TWIC cards to a significantly larger population of workers in a timely manner than was done during testing of the TWIC program. In testing the TWIC program, TSA enrolled and issued TWIC cards to only about 1,700 workers, short of its goal of 75,000 workers. According to TSA and the testing contractor, lack of volunteers to enroll in the TWIC program during testing and technical difficulties in enrolling workers, such as problems obtaining workers' fingerprints to conduct background checks, led to fewer than expected enrollments during testing. TSA officials stated that the agency is using the testing experience to make improvements to the enrollment and card issuance process, which should address these problems during TWIC implementation. For example, TSA plans to use an easier and faster form of scanning to capture workers' fingerprints and is taking additional steps to ensure that the process for enrolling workers and issuing TWIC cards is efficient. Taking these steps should help TSA to address the problems experienced during TWIC testing. While these actions should address the problems that occurred during testing, during implementation, TSA faces the challenge of enrolling and issuing TWIC cards to 750,000 workers at 3,500 maritime facilities and 10,800 vessels—a significantly larger population of workers. The second challenge will be ensuring that the access control technology required to operate the TWIC program, such as biometric card readers, works effectively in the maritime sector. Few facilities that tested the TWIC program used biometric card readers that will be required when the program is implemented. As a result, TSA has obtained limited information on the operational effectiveness of biometric readers, particularly when individuals use these readers outdoors in the harsh maritime environment. In addition, most testing facilities lacked the technology to connect with TSA's national TWIC database to obtain current information on those workers already issued TWIC cards who have subsequently been identified as a potential threat to security or whose cards have been lost or stolen. TSA's recent decision to implement the TWIC program by issuing two separate rules will give the agency more time to consider maritime industry concerns regarding TWIC access control technologies and develop solutions to address these problems that will help ensure that TWIC will work effectively in the maritime

environment. However, TSA officials stated that the agency does not plan to conduct additional testing of TWIC access control technologies to ensure that they work effectively before the program is implemented. DHS plans to finalize the initial TWIC rule, which will include enrolling workers, conducting background checks, and issuing TWIC cards, by the end of calendar year 2006. According to TSA, the agency will also issue a subsequent proposed rule requiring the installation of TWIC access control technologies at a future date. As a result, TWIC cards will initially be used as a photo identification to enter secure areas until additional requirements for access control technologies are finalized by TSA**.** The third challenge DHS faces is balancing the added security benefits of the TWIC program in preventing a terrorist attack that could result in a costly disruption in maritime commerce with the impact that the program could have on the daily flow of maritime commerce. For example, if an individual worker or truck driver has problems with his or her fingerprint verification on a biometric card reader, it could create a long queue, delaying other workers and trucks waiting in line trying to enter secure areas of a port. TSA and the Coast Guard have acknowledged the potential impact that the TWIC program could have on the flow of maritime commerce and, as a result, plan to obtain additional comments on this issue from industry stakeholders in the second rulemaking pertaining to access control technology. Given the large investment required by the federal government and maritime industry to implement the TWIC program, it is important that solutions to these problems are developed and tested prior to implementation to help ensure that the program meets its intended goals without further delays and that government and maritime industry resources are used efficiently.

TSA experienced problems in planning for and overseeing the contract to test the TWIC program. Specifically, poor planning resulted in significant contract changes shortly after TSA awarded the contract, which contributed to a doubling of contract costs. According to TSA officials, delays in program development and pressure to begin TWIC testing caused the agency to award the contract before they had sufficient time to plan for and identify all of the requirements necessary to test the TWIC program in the initial contract. For example, TSA had to amend the initial contract to require the contractor to install the access control infrastructure necessary to test the TWIC program at facilities. In addition, TSA did not effectively oversee the contractor's performance to ensure that all key components of the TWIC program were tested. For example, TSA did not follow its contract oversight guidance in certain areas, including performing its own evaluation of the contractor's performance. In addition, a report by an independent contractor found that 25 percent of

the operational and performance requirements in the testing contract were not met, such as the requirement that lost or stolen TWIC cards be revoked before a transportation worker is issued a new TWIC card. The independent contractor's assessment characterized the failure to meet this specific requirement as a critical problem, because a terrorist could potentially use the lost or stolen card to attempt to gain access to secure areas of transportation facilities. TSA officials told us they did not have enough personnel to provide effective oversight of the contract to test the TWIC program and relied on the contractor to provide oversight of its own work and the work of its subcontractors. In addition to oversight problems, stakeholders at all 15 TWIC testing locations we visited told us that TSA did not effectively communicate and coordinate with them regarding any problems that arose during testing at their facility. TSA officials acknowledged that the agency could have better communicated with stakeholders at the TWIC testing locations. The problems we identified are consistent with those discussed in previous GAO reports, such as poor contract planning, oversight, and communication and coordination at TSA and DHS. Specifically, we previously reported that TSA did not adequately ensure that contract requirements and deliverables were clearly defined and did not provide adequate oversight of contractor performance, which increased contract costs. According to TSA officials, the agency has taken steps to address these contract planning and oversight problems by hiring additional staff with program management and technical expertise to assist in developing contract requirements and providing oversight of the future contract to implement the TWIC program. However, it is not clear to what extent these actions will ensure that the contract to implement the TWIC program will include comprehensive and clearly defined contract requirements and that contractor performance will be closely monitored to ensure that the program is implemented successfully and costs are controlled.

To help ensure that the TWIC program can be implemented as efficiently and effectively as possible, we are recommending two actions. First, we recommend that, before TSA begins implementing TWIC in the maritime sector, the agency develop and test solutions to the problems identified during TWIC program testing and raised by stakeholders in commenting on the TWIC proposed rule to help ensure that all key components of the TWIC program work effectively. Second, TSA should strengthen contract planning and oversight practices before awarding the contract to implement the TWIC program.

We provided a draft of this report to DHS for review. DHS, in its written comments, concurred with the findings and recommendations in the report. The full text of DHS's comments is included in appendix II.

Background

Securing transportation systems and facilities is complicated, requiring balancing security to address potential threats while facilitating the flow of people and goods. These systems and facilities are critical components of the U.S. economy and are necessary for supplying goods throughout the country and supporting international commerce. U.S. transportation systems and facilities move over 30 million tons of freight and provide approximately 1.1 billion passenger trips each day. The Ports of Los Angeles and Long Beach estimate that they alone handle about 43 percent of the nation's oceangoing cargo. The importance of these systems and facilities also make them attractive targets to terrorists. These systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and close proximity to urban areas. A terrorist attack at these systems and facilities could cause a tremendous loss of life and disruption to our society. An attack would also be costly. According to recent testimony by a Port of Los Angeles official, a 2002 labor dispute led to a 10-day shutdown of West Coast port operations, costing the nation's economy an estimated $1.5 billion per day.[6] A terrorist attack to a port facility could have a similar or greater impact.

One potential security threat stems from those individuals who work in secure areas of the nation's transportation system, including seaports, airports, railroad terminals, mass transit stations, and other transportation facilities. It is estimated that about 6 million workers, including longshoreman, mechanics, aviation and railroad employees, truck drivers, and others access secure areas of the nation's estimated 4,000 transportation facilities each day while performing their jobs. Some of these workers, such as truck drivers, regularly access secure areas at multiple transportation facilities. Ensuring that only workers that do not pose a terrorist threat are allowed unescorted access to secure areas is important in helping to prevent an attack. According to TSA and transportation industry stakeholders, many individuals that work in secure areas are currently not required to undergo a background check or a

[6] Testimony of the Director of Homeland Security, Port of Los Angeles, before the United States Senate Committee on Commerce, Science, and Transportation, May 16, 2006.

stringent identification process in order to access secure areas. For example, according to stakeholders at several ports, truck drivers need only present a driver's license, which can be easily falsified and obtained, to access secure areas of the nation's ports. In addition, without a standard credential that is recognized across modes of transportation and facilities, many workers must obtain multiple credentials to access each transportation facility they enter. For example, in Florida, truck drivers who deliver goods to multiple ports in the state must obtain credentials for as many as 13 individual ports. With so many different credentials in use, it may be difficult to verify the authenticity of all of them.

TWIC Program History

In the aftermath of the September 11, 2001, terrorist attacks, the Aviation and Transportation Security Act (ATSA) was enacted in November 2001. Among other things, ATSA required TSA to work with airport operators to strengthen access control points in secure areas and consider using biometric access control systems 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 to mitigate the threat of terrorists and other unauthorized persons from accessing secure areas of the entire transportation network, by creating a common identification credential that could be used by workers in all modes of transportation. In November 2002, the Maritime Transportation Security Act of 2002 (MTSA) was enacted and required the Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels, among other things.

The responsibility for securing the nation's transportation system and facilities is shared by federal, state, and local governments, as well as the private sector. At the federal government level, TSA, the agency responsible for the security of all modes of transportation, has taken the lead in developing the TWIC program, while the Coast Guard is responsible for developing maritime security regulations and ensuring that maritime facilities and vessels are in compliance with these regulations. As a result, TSA and the Coast Guard are working together to implement TWIC in the maritime sector. According to TSA officials, TWIC is being implemented in the maritime sector first to meet MTSA requirements and because the aviation sector already has established systems to control access to secure areas. According to TSA, the agency is considering extending the program to other modes of transportation. Most seaports, airports, mass transit stations, and other transportation systems and facilities in the United States are owned and operated by state and local

government authorities and private companies. As such, certain components of the TWIC program, such as installing access control systems, such as card readers, will be the responsibility of these state and local governments and private industry stakeholders. For example, at most seaports, the private companies that operate the terminal are responsible for controlling access to secure areas, while at other ports, local governments handle this responsibility. As a result, the responsibility for implementing certain components of the TWIC program at each facility will be shared between local governments and the private sector.

TSA—through a private contractor—tested the TWIC program from August 2004 to June 2005 at 28 transportation facilities around the nation, including 22 port facilities, 2 airports, 1 rail facility, 1 maritime exchange, 1 truck stop, and a U.S. postal service facility. In August 2005, TSA and the testing contractor completed a report summarizing the results of the TWIC testing. TSA also hired an independent contractor to assess the performance of the TWIC testing contractor. Specifically, the independent contractor conducted its assessment from March 2005 to January 2006, and evaluated whether the testing contractor met the requirements of the testing contract. The independent contractor issued its final report on January 25, 2006.

Since its creation, the TWIC program has received about $90 million in funding for program development and testing. Table 1 provides a summary of TWIC program funding since fiscal year 2003.

Table 1: TWIC Program Funding from FY 2003 to FY 2006 (Dollars in millions)

Fiscal Year	Appropriated	Reprogramming/transfers	Total funding
2003	$25.0	($5.0)	**$20.0**
2004	$49.7	0	**$49.7**
2005	$5.0	0	**$5.0**
2006	0	$15.0	**$15.0**
Total	**$79.7**	**$10.0**	**$89.7**

Source: TSA.

Note: TSA's fiscal year 2007 congressional justification includes $20 million in authority to collect fees from transportation workers for TWIC cards.

In December 2004, we reported on the challenges TSA faced in implementing the TWIC program, such as developing regulations and a comprehensive plan for managing the program.[7] We also reported on several factors that caused TSA to miss its initial August 2004 target date for issuing TWIC cards, including (1) difficulty obtaining approval from DHS to test the TWIC program; (2) delays in developing cost-benefit and alternative analyses for the program; and (3) difficulty determining which TWIC card technologies were best suited for the port environment. We recommended that TSA employ industry best practices for project planning and management by developing a comprehensive project plan for managing the program and specific detailed plans for risk mitigation and cost-benefit and alternatives analyses. DHS generally agreed with these recommendations and subsequently developed plans to help them manage the TWIC program, ensure quality, and assess and mitigate the risks to the program. According to TSA, the agency also developed a cost model to assist in developing program budget estimates.

Key Components of TWIC Program

According to TSA, the TWIC program, under the proposed rule issued in May 2006, is to consist of key components designed to enhance security (see fig. 1). These include:

- **Enrollment:** Transportation workers are to be enrolled in the TWIC program at enrollment centers by providing personal information, such as a social security number and address, digital photographs, and fingerprints. Workers who are unable to provide quality fingerprints are to provide an alternate authentication mechanism, such as a digital photograph.

- **Background checks:** TSA is to conduct background checks on each worker to ensure that individuals do not pose a threat. These are to include several components. First, TSA is to conduct a security threat assessment to make sure that the worker is not listed in any terrorism databases or on a terrorism watch list, such as TSA's No-fly and selectee list. Second, a Federal Bureau of Investigation criminal history records check is to be conducted to identify if the worker has any disqualifying criminal offenses. Third, workers immigration status is to be checked by the U.S. Citizenship and Immigration Service. Workers

[7] GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: December 2004).

are to have the opportunity to appeal the results of the background check or request a waiver if they do not pass the check.

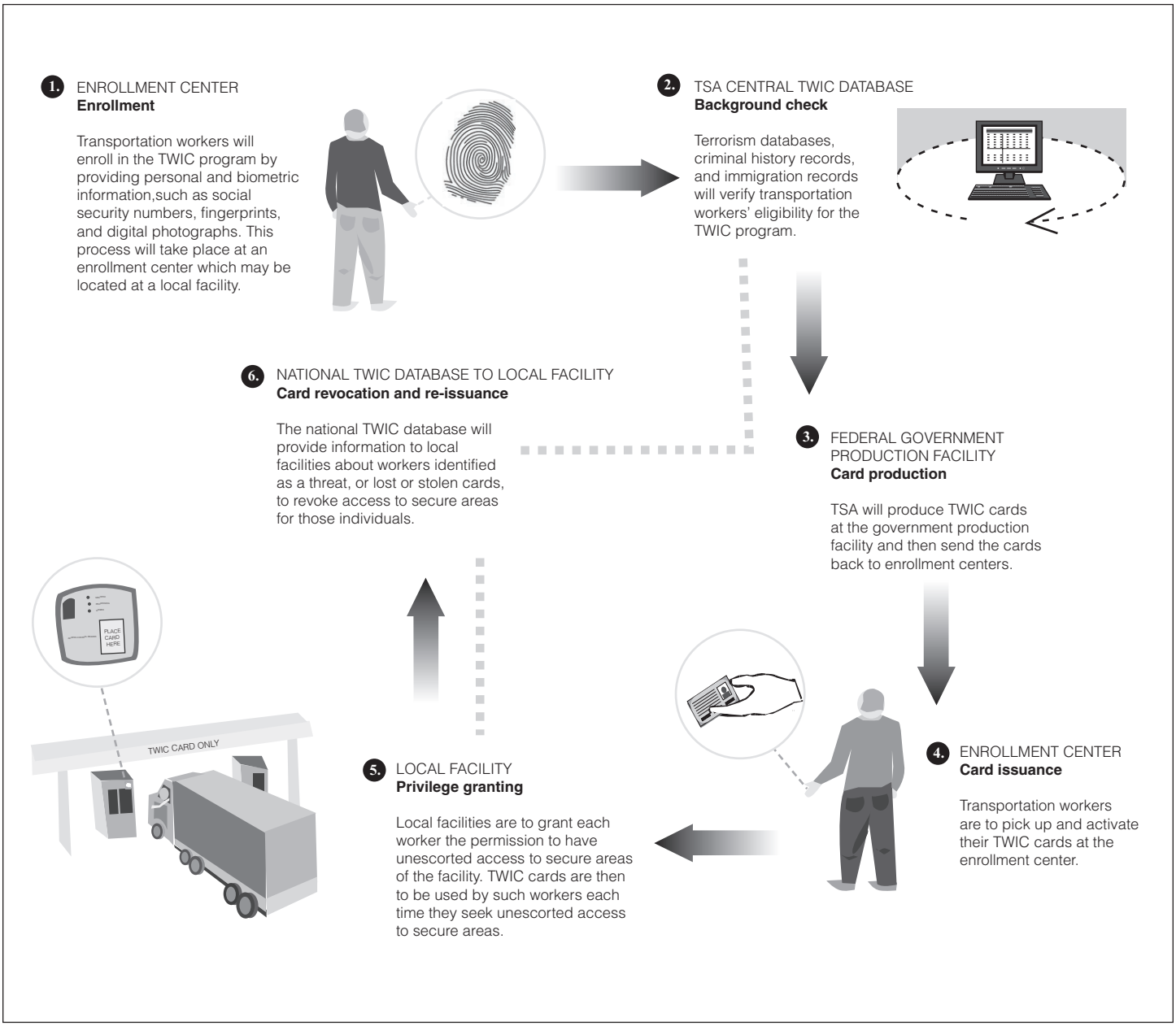
- **TWIC card production:** After TSA determines that a worker has passed the background checks, the agency provides transportation worker information to a federal card production facility where the TWIC card is to be personalized for the worker, manufactured, and then sent back to the enrollment center.

- **Card issuance:** Transportation workers are to be informed when their cards are ready to be picked up at enrollment centers.

- **Privilege granting:** TWIC cards are to be activated at enrollment centers and workers will choose a personal identification number. Transportation facility security officials will then grant workers access to secure areas on an individual basis. Workers are to then use their TWIC cards to match the card to the card holder when accessing secure areas through biometric access control systems.

- **Card Revocation:** Local facilities can download or receive real-time lists of workers deemed to pose a threat or whose cards have been lost or stolen from TSA. Facilities can then remove these workers' access privileges to secure areas. TWIC cards are to be renewed and background checks repeated every 5 years. Cards will be re-issued to workers if ever lost or stolen.

Figure 1: Overview of the TWIC Process Under the TWIC Proposed Rule



Source: GAO analysis of TSA information.

TWIC Proposed Rule for Maritime Sector

In May 2006, DHS issued a proposed rule that describes the requirements of the TWIC program that the owners and operators of maritime facilities and vessels would be required to implement.[8] Table 2 provides an overview of the requirements in the TWIC proposed rule.

Table 2: Requirements of the TWIC Proposed Rule

Proposed requirement	Description of proposed requirement
Transportation workers	Individuals who require unescorted access to secure areas of MTSA regulated vessels, facilities, and outer continental shelf (OCS) facilities and all U.S. Coast Guard credentialed merchant mariners must obtain a TWIC card.
Facility, vessel, and OCS facility security plans	All facilities, vessels, and OCS facilities currently regulated by MTSA must create a TWIC addendum to current security plans within 6 months of the final TWIC rule being published and be operating under this plan within 12-18 months.
Background checks	All workers applying for a TWIC card must provide biographic information and fingerprints to TSA to conduct a security threat assessment, undergo a FBI fingerprint based criminal history records check, and undergo an immigration status check. The proposed rule requires all workers applying for a TWIC card to provide fingerprints and a digital photograph. Digital photographs are to be used as the alternate biometric for individuals who are unable to provide fingerprints at the time of card issuance. In order to receive a TWIC, workers must not pose a security threat and must not have committed a disqualifying criminal offense.
Appeals and waiver process	All TWIC applicants will have opportunity to appeal the results of the background check to correct cases of mistaken identity or inaccurate court records. In addition, applicants that are disqualified due to previous criminal activity or mental incapacity may apply for a waiver.
Access control systems	Each facility, vessel, and OCS facility is required to have access control systems and equipment, including card readers, that meet TSA approved standards and Federal Information Processing Standard (FIPS) 201. Card readers must be able to verify biometrics and include the capability to enter a personal identification number.
Access to secure areas	Each facility, vessel, and OCS facility may allow only persons who hold a TWIC to have unescorted access to secure areas of the facility or vessel and are responsible for ensuring that TWIC cards are valid, unless revoked.
Checking the validity of TWIC cards	Each facility, vessel, and OCS facility must verify that a worker's TWIC card is valid, either by directly interfacing with TSA's national TWIC database or using a list of invalid credentials downloaded from TSA. TWIC cards will be valid for 5 years.

Source: GAO analysis of TSA and Coast Guard proposed rule on TWIC.

[8] Under the joint rulemaking TSA would amend current transportation security regulations in title 49 Code of Federal Regulations (CFR) to include the overall components of the TWIC program and the Coast Guard would amend current maritime security regulations in title 33 CFR and title 46 CFR to include the process for implementing TWIC at MTSA regulated facilities and vessels as well as how these facilities and vessels should amend current security plans. In addition, a second Coast Guard rulemaking designed to streamline the existing merchant mariner credentialing process would amend merchant mariner credentialing requirements in title 33 CFR and title 46 CFR.

In the TWIC proposed rule, TSA and the Coast Guard present cost estimates for implementing the TWIC program. According to the estimates, the cost of the TWIC program to the federal government and the maritime industry could range from about $777 million to $829 million over the next 10 years.[9] About 40 percent of these costs—$355 million to $378 million—would be incurred in the initial program start up. According to TSA and the Coast Guard's cost estimate, about 48 percent of the total cost of the TWIC program will be incurred by the owners and operators of port facilities and vessels. TSA and the Coast Guard estimate that the total cost to these facilities and vessel owners and operators will be about $467 million over 10 years, mostly for the installation of access control systems and other technology to operate these systems. In addition to these costs, TSA and the Coast Guard estimate that they will charge a fee of $149 to produce and issue each TWIC card for the estimated 750,000 workers that will need to receive a card. According to TSA, this fee will cover the cost of the background checks and card production and issuance. This fee is to be collected from the applicant at the enrollment center when applying for a TWIC.

In August 2006, DHS decided that the TWIC program would be implemented in the maritime sector using two separate rules, one for enrolling workers and issuing cards and the second for implementing TWIC access control technologies, such as biometric card readers. DHS made the decision to use two separate rules in response to numerous maritime industry concerns about whether the access control technologies necessary to operate the TWIC program will work effectively in the maritime sector. DHS plans to finalize the first TWIC rule, which is expected to cover enrolling workers, conducting background checks, and issuing TWIC cards, by the end of calendar year 2006. TWIC access control technology requirements are expected to be addressed in a second TWIC proposed rule, to be issued after DHS finalizes the first TWIC rule.

[9] These costs are estimated in present value dollars discounted at 7 percent.

DHS and Industry Stakeholders Face Challenges in Addressing Testing Problems and Ensuring Key Components of the TWIC Program Work Effectively

DHS and industry stakeholders face three major challenges in addressing problems identified during TWIC program testing and ensuring that key components of the TWIC program can work effectively. The first challenge is enrolling and issuing TWIC cards to a significantly larger population of workers in a timely manner than was done during testing of the TWIC program. The second challenge will be ensuring that the technology required to operate the TWIC program, such as biometric card readers, works effectively in the maritime sector. The third challenge DHS faces is balancing the added security benefits of the TWIC program in preventing a terrorist attack that could result in a costly disruption in maritime commerce with the impact that the program could have on the daily flow of maritime commerce. TSA and Coast Guard officials told us they are taking steps to improve the enrollment and card issuance process, and plan to obtain additional comments on the access control technology requirements for the TWIC program and the potential impact that the program could have on the flow of maritime commerce as part of a second rulemaking on the TWIC program. Given the large investment required by the federal government and maritime industry to implement the TWIC program, it is important that solutions to these problems are developed and tested prior to implementation to help ensure that the program meets its intended goals without further delays and that government and maritime industry resources are used efficiently.

TSA Has Improved TWIC Enrollment and Card Issuance Processes, but Faces Challenges in Enrolling Significant Numbers of Workers During Implementation

TSA had difficulty in meeting its goals for enrolling workers and issuing TWIC cards during testing. Specifically, TSA's goal was to enroll and issue TWIC cards to 75,000 workers at 28 transportation facilities. However, only about 12,900 workers were enrolled and only about 1,700 TWIC cards were issued to workers at 19 facilities. According to TSA officials and the testing contractor, these problems were caused by difficulties finding volunteers to enroll in the TWIC program during testing and technical problems, such as collecting fingerprints from workers at certain testing locations and enrolling large numbers of workers at one time. TSA officials stated that during implementation the agency will use a faster and easier method of collecting fingerprints and will enroll workers individually. While these actions should address the problems that occurred during testing, during implementation, TSA faces the challenge of enrolling and issuing TWIC cards to 750,000 workers at 3,500 maritime facilities and 10,800 vessels—a significantly larger population of workers than were included in TWIC program testing.

Another challenge TSA faces is ensuring that workers are not providing false information and counterfeit identification documents when they enroll in the TWIC program. This step is of critical importance in ensuring

that a person being issued a TWIC card does not pose a security threat. Since social security cards, immigration documents, passports, and other forms of identification can be obtained from fraudulent identity providers, the authenticity of these documents must be verified and personnel that enroll workers must be trained to identify fraudulent documents. During TWIC testing, enrollment personnel were provided some training in identifying fraudulent documents. According to TSA, the TWIC enrollment process to be used during implementation will include using document scanning and verification software to help determine if identification documents are fraudulent and training personnel to identify fraudulent documents. While it is important that the enrollment process include the capability to prevent workers from using fraudulent identification documents to obtain a TWIC card, details on the approach that TSA will use during implementation are not yet available.

In addition, TSA is taking steps to address other problems regarding enrolling workers and issuing TWIC cards in a timely manner that were encountered during testing. Specifically, TSA has eliminated approaches used at certain locations to collect fingerprints and enroll large groups of workers at one time, which caused problems during testing, and kept approaches to enrolling workers and issuing cards that worked successfully at other locations. While these actions appear to address these problems, TSA could not provide us the results of how these successful approaches worked at other testing locations.

Figure 2 is an example of an enrollment station used during testing of the TWIC program.

Figure 2: TWIC Enrollment Station Used during Testing

Source: GAO.

Industry Stakeholders Face Obstacles in Implementing TWIC Access Control Technology and Ensuring That It Works Effectively during Implementation

The TWIC proposed rule would require each facility and vessel to (1) install and use biometric card readers in the maritime environment to control access to secure areas, (2) link these card readers to the individual facility or vessel access control system, or use hand held card readers, and (3) routinely connect to TSA's national TWIC database and incorporate updates on TWIC cards that should be revoked because a worker poses a security threat or a TWIC card has been lost or stolen. Our analysis of the results of TWIC program testing and visits to 15 of the 28 testing sites, as well as the concerns expressed by industry stakeholders at public meetings on the TWIC proposed rule, suggest that it may be difficult to implement each of these steps. Furthermore, industry stakeholders are concerned about the cost of implementing and operating biometric card readers, linking the readers to their local access control system, and connecting to TSA's national TWIC database. TSA's recent decision to implement the TWIC program by issuing two separate rules will give the agency more time to consider maritime industry concerns regarding the TWIC access control technology and develop solutions that will help ensure that TWIC will work effectively in the maritime environment. TSA

is also working with the National Institute of Standards and Technology (NIST) to ensure that the biometric identification cards and card readers to be used for the TWIC program meet federal standards for identification and access controls. [10]

Problems with Installing and Using Biometric TWIC Card Readers

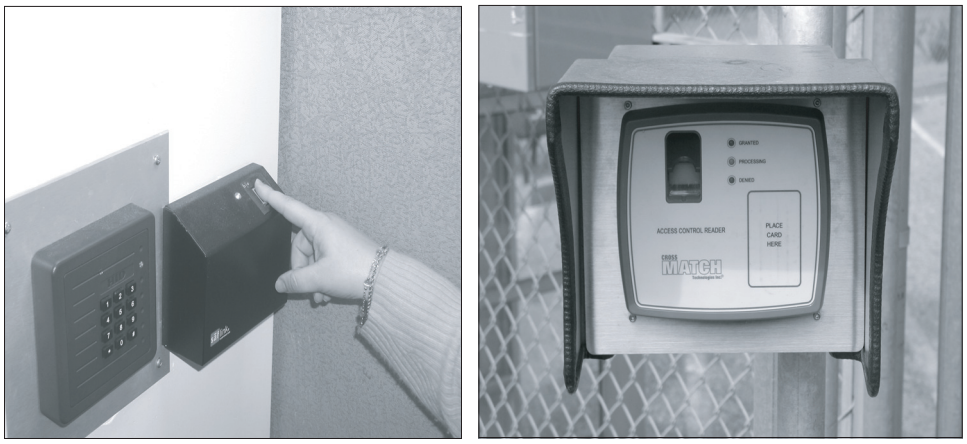
Industry stakeholders will be required to install biometric TWIC card readers capable of reading a worker's fingerprint and matching that fingerprint to a worker's TWIC card in order for the worker to gain unescorted access to secure areas of a facility or vessel. While TSA was able to provide us the total number of card readers installed at each testing location, they could not tell us which or how many of these card readers were biometric or non-biometric. According to TWIC testing contractor officials, less than half of the 99 card readers installed during TWIC testing were biometric. In addition, only 8 of the 15 testing facilities that we visited tested biometric card readers, and officials at only 2 of these 8 facilities told us that their biometric card readers functioned effectively. For example, at one testing facility, six biometric card readers were installed, but were never operational because the testing contractor had difficulty installing the infrastructure to provide electrical power and communications capability to the readers themselves. As a result, the biometric card readers were never used by workers at this facility. According to TSA officials, the agency and the testing contractor did not have the authority or responsibility for installing or repairing facility access control systems and infrastructure during TWIC testing, other than what was agreed to in the initial memorandum of understanding with those facilities.

In addition, TSA did not test the use of biometric card readers on vessels at all during testing of the TWIC program, although the TWIC proposed rule requires the use of biometric card readers on vessels during implementation of the program. An independent assessment of TWIC testing also found that 10 of the 18 TWIC testing sites they visited encountered problems installing TWIC technologies. Although the independent assessment does not specify the problems encountered, TSA and the TWIC testing contractor confirmed that some sites had problems installing the infrastructure necessary to operate the TWIC card readers

[10] On August 27, 2004, the President signed and issued Homeland Security Presidential Directive (HSPD) 12, which establishes a common identification standard, including standards for biometrics, for federal employees and federal contractors. Shortly after HSPD 12 was signed, NIST issued Federal Information Processing Standard (FIPS) 201 to provide guidance and standards for complying with HSPD 12.

and others had problems effectively interfacing card readers with existing facility access control systems. Figure 3 provides an example of biometric card readers used during testing of the TWIC program.

Figure 3: Fingerprint Based Biometric Card Readers Used during TWIC Testing



Source: GAO.

In commenting on the TWIC proposed rule, industry stakeholders expressed concerns regarding TSA's limited testing of biometric card readers and the challenges of using these readers in the harsh outdoor maritime environment. Stakeholders that have already installed biometric fingerprint-based card readers in the outdoor maritime environment stated that these readers did not work effectively in the maritime environment where they were often damaged and affected by dirt, wind, salt, and water. Several stakeholders also provided comments about the design of TWIC card readers to ensure that these readers were less susceptible to the elements in the maritime environment, such as salt and water. In addition, the TWIC testing contractor recommended that contactless card readers be used during implementation of the TWIC program to more quickly process workers into secure areas and better withstand the harsh maritime environment. According to TSA, the agency will consider these and other industry stakeholder comments regarding TWIC access control technologies as part of the second rulemaking.

Several industry stakeholders proposed that TSA conduct additional maritime testing of biometric card readers, including their use on vessels, to provide assurance that the TWIC program technology works effectively before it is implemented nationwide and ensure that their investments in this technology and infrastructure would be worthwhile. Stakeholders also

suggested that TSA and the Coast Guard closely coordinate with maritime stakeholders that have implemented or are currently using biometric access control systems. For example, Florida is currently implementing a statewide uniform port access biometric credential program, similar to the TWIC program. Coordinating with Florida and other stakeholders could enable TSA and the Coast Guard to learn from these stakeholders' experiences and potentially test key components of the TWIC program and develop solutions to the various implementation challenges identified during testing.

As discussed earlier, in August 2006, DHS decided that the TWIC program would be implemented using two separate rules, one for enrolling workers and issuing cards and the second for implementing TWIC access control technologies, such as biometric card readers. DHS made this decision following numerous maritime industry comments about whether the access control technologies necessary to operate the TWIC program will work effectively. According to TSA, the agency is working with NIST to ensure that the biometric identification cards and card readers to be used for the TWIC program meet federal standards for identification and access controls. We requested additional information from TSA on the time frames on the second TWIC rulemaking and how this rulemaking will ensure that TWIC access control technologies, such as biometric card readers, will work effectively in the maritime environment. TSA officials told us that they could not provide us any details about the second rulemaking. As a result, it is not clear how the TWIC cards will initially be used to permit workers to enter secure areas without requirements for TWIC access control technologies, such as biometric card readers.

Difficulties in Linking Biometric Card Readers to Facility Access Control Systems

Under the TWIC proposed rule, maritime facility and vessel owners and operators would be responsible for installing biometric card readers and linking them to individual facility or vessel access control systems, to ensure that only those with valid TWIC cards, who have been granted access rights by the facility, have unescorted access to secure areas. According to the TWIC testing contractor's report, only 10 of the 28 TWIC testing facilities linked card readers to the local facility access control system. The report did not specifically discuss the effectiveness of the link between card readers and the facility access control system at these 10 locations. TSA said it was unable to identify the specific testing locations where card readers were linked to local access control systems or any additional results regarding the link between card readers and access control systems. According to TSA and the testing contractor, they encountered difficulties in linking card readers to access control systems during testing because many facilities lacked the infrastructure necessary

to do so. For example, TSA and testing contractor officials told us that at most maritime facilities participating in testing, electrical power supplies and high-speed communications lines were not available at all of the access control points where card readers were needed, especially those far away from the facility's central access control system. As a result, linking card readers to the access control system would have been too difficult and costly to perform during testing. In addition, because TSA did not install TWIC card readers on vessels during testing, the agency did not test the link between card readers and vessel access control systems.

Industry stakeholders have expressed concern that TSA conducted only limited testing of the link between biometric card readers and local facility access control systems. In addition, the difficulties encountered by the TWIC testing contractor in establishing this link raises questions about the difficulty in doing so during TWIC implementation. For example, some stakeholders stated that they tried but were unable to link biometric card readers to the computers and computer software running their current access control systems. An official at one testing facility told us that his facility spent its own money to hire a technology integrator to link TWIC card readers to the facility access control system because TSA and the testing contractor did not do so during testing of the TWIC program.[11] Stakeholders also expressed concerns that the new biometric TWIC card readers will not be compatible with their existing access control systems and as a result, they will incur additional costs if they are required to purchase new access control systems. According to TSA, while facility and vessel owners and operators will be required to install TWIC card readers, it is up to these facilities and vessels whether they want to link these card readers to their access control systems. TSA recently announced that requirements for purchasing and installing card readers will not be implemented until the public is afforded additional time to comment on that aspect of the TWIC program and the details of this approach will be explained in the next rulemaking.

TSA Did Not Test the Connection of Local Facilities to the National TWIC Database

A key security component of the TWIC program is the ability to quickly revoke a worker's unescorted access privileges to secure areas if TSA identifies a worker as a security threat or if the worker's TWIC card is lost or stolen. This requires that (1) TSA identify that a worker is a threat to

[11] During testing of the TWIC program, TSA and the testing contractor did install some technology and infrastructure necessary to test the TWIC program. However, according to the TWIC proposed rule, facilities and vessels will be responsible to installing technology and infrastructure during implementation.

security or that their card has been lost or stolen and invalidate their TWIC card from the national TWIC database; (2) TSA quickly communicates information to facilities regarding those workers whose TWIC cards have been invalidated; and (3) the facility removes a worker's access privileges to secure areas from their local access control system. However, according to TSA, the testing contractor encountered problems in connecting the national TWIC database to local facilities' access control systems during testing of the TWIC program. As a result, TSA did not test this connection at any of the 28 testing locations. Several TWIC testing facilities that we visited lacked the technology, such as computer systems and high-speed communications lines, to connect with TSA's national TWIC database to obtain information on workers that may pose a potential threat or whose TWIC cards had been lost or stolen. An independent contractor's assessment of the testing also found that TSA did not test the connection between the national TWIC database and local facility access control systems. The independent assessment characterized this as a critical failure because a worker posing a threat could access secure areas of a facility if that facility had not been informed that TSA revoked his or her TWIC card. TSA officials stated that, while they did not test the connection between the national TWIC database and facilities in the field, they tested this component in a laboratory. However, TSA officials said they were unable to provide any reports on this laboratory testing. According to TSA officials, under the TWIC proposed rule, this problem will be resolved because facilities and vessels can download updates from the national TWIC database on a regular basis regarding workers who pose a threat as an alternative to directly connecting with the national database. Since this approach was not used during TWIC program testing, it is important that it be tested to ensure that it works effectively during implementation.

The TWIC proposed rule requires that each facility and vessel have the capability to verify that a worker that has been issued a TWIC card has not subsequently been identified by TSA as a threat and that a TWIC card has not been lost or stolen. The proposed rule allows facilities and vessels the option of directly interfacing with TSA's national TWIC database or routinely downloading a list of invalid TWIC cards from TSA through a

secure Web site.[12] In commenting on the TWIC proposed rule, numerous stakeholders expressed confusion about how to connect to TSA's national TWIC database and what technology they will need to do so.[13] Stakeholders participating in TWIC program testing also expressed concern that TSA did not test this connection at any of the TWIC testing locations. In addition, some stakeholders were concerned about how vessels at sea without internet or satellite service would connect with the national TWIC database to get updates regarding workers who pose a threat or whose TWIC cards have been lost or stolen because TSA also did not test this connection. According to TSA, these issues will be addressed as part of the second rulemaking on TWIC access control technologies.

Industry Stakeholders Concerned about the Cost and Security of TWIC Program Technology

In addition to concerns about whether or not the access control technology will work effectively in the maritime environment, facility and vessel owners and operators are also concerned about the cost and security of technology necessary to implement the TWIC program. TSA and the Coast Guard estimate that, on average, a maritime facility will spend $90,000 per facility to upgrade or install access control systems, including biometric card readers. However, in commenting on the TWIC proposed rule, stakeholders stated that they believe that upgrading and installing access control systems at maritime facilities will cost much more than the TSA and the Coast Guard estimate. For example, one port facility has 37 individual terminals, several of which could require 20 or more card readers for entry and exit lanes at one terminal alone. Port officials estimated that it could cost up to $300,000 per terminal to install the necessary TWIC card readers. Several stakeholders are also concerned that TSA and the Coast Guard cost estimates do not take into account the facilities' costs to maintain equipment and technology, such as card readers, or the cost to hire additional staff needed to perform such maintenance. Facility and vessel owners also stated that the cost of installing TWIC card readers and other equipment necessary to use TWIC

[12] According to the TWIC proposed rule, at maritime security (MARSEC) level 1, the facilities and vessels would be required to ensure that the validity of TWIC credentials are verified against the latest information available from TSA on a weekly basis. At MARSEC level 2, facilities and vessels would be required to ensure the validity of TWICs on a daily basis. At MARSEC level 3, all personnel seeking unescorted access would be required to verify their identity biometrically and use their PIN at each entry to a secure area of the facility or vessel.

[13] The proposed rule offers facilities and vessels the option of downloading lists of invalid cards or workers that pose a threat through a secure TSA Web site instead of directly interfacing with the national TWIC database. However, it does not provide details on the specifics of this process.

may be a hardship for smaller facilities and vessel operators. We requested additional information on how TSA and the Coast Guard developed the cost estimates in the proposed rule, however, DHS could not provide this information. As a result, we were unable to determine if these estimates were reasonable.

Further, industry stakeholders are concerned about the security of the personal information given to TSA to conduct TWIC background checks. For example, stakeholders commenting on the TWIC proposed rule questioned how TSA will ensure the security of workers' information in light of the fact that other government agencies have mishandled and lost private personal information. In an August 2006 report, the DHS Inspector General highlighted shortcomings in information security for the TWIC program.[14] According to the report, TSA faces numerous challenges in ensuring that security vulnerabilities—which could compromise the confidentiality, integrity and availability of sensitive TWIC data—are remedied and key program policies, regulatory processes, and other work are completed to support the full implementation of the TWIC program.[15] According to the report, TSA agreed with these findings and plans to take steps to correct the security concerns identified.

DHS Recognizes Stakeholder Concerns Regarding TWIC Implementation, but Plans No Further Program Testing

DHS officials acknowledged that there are challenges in ensuring that the TWIC technology works effectively in a maritime environment. Accordingly, DHS decided in August 2006 that it will not require maritime facilities and vessels to implement TWIC card readers and other TWIC access control technologies until the maritime industry has additional time to comment on these aspects of the program. However, TSA is not planning to conduct any additional testing of TWIC program technologies.

TSA officials said that the agency is working with NIST to ensure that the biometric identification cards and card readers to be used for the TWIC

[14] Department of Homeland Security, OIG-06-47: *DHS Must Address Significant Security Vulnerabilities Prior to TWIC Implementation*, August 2006.

[15] The Inspector General attempted to determine whether adequate system security controls have been implemented on TWIC systems to protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. The Inspector General audited information security management and access controls implemented for the systems supporting the TWIC program testing and found that significant security vulnerabilities exist related to the TWIC testing systems, documentation, and program management and there are a number of program and security-related concerns.

program meet federal standards for identification and access controls. Specifically, these standards concern the use of biometric identification and access control systems for federal employees and contractors. According to TSA, although these standards are not specifically directed at the TWIC program, the agency believes it is important for the program to comply with these standards. However, NIST's review of the TWIC program does not involve any actual testing of the TWIC program technology, such as the use of biometric card readers in a maritime environment.

Ensuring That the TWIC Program Balances Security and the Flow of Maritime Commerce May Be Difficult

In addition to ensuring that key components of the TWIC program work effectively, another challenge DHS faces is balancing the added security components of the TWIC program with the potential effect that the program could slow the daily flow of maritime commerce. If implemented effectively, the security benefits of the TWIC program in preventing a terrorist attack could save lives and avoid a costly disruption in maritime commerce. Alternatively, if key components of the TWIC program, such as biometric card readers, do not work effectively, it could slow the daily flow of maritime commerce. Our discussions with industry stakeholders at facilities that participated in TWIC testing and stakeholder comments on the TWIC proposed rule identified four concerns about the potential impact of TWIC on maritime commerce.

Wait Times to Receive TWIC Cards

According to stakeholders, for the TWIC program to work effectively in the maritime environment without slowing commerce, TWIC cards must be issued within a few days after enrollment, or workers should be allowed interim access to secure areas to perform their job duties while they wait to receive a TWIC card. Several maritime facility officials stated that without quick issuance or interim access, they will have difficulty in staffing and performing operations. Some passenger vessel owners and operators stated that waiting 30 to 60 days to receive a TWIC card could hinder their ability to allow workers to access secure areas to perform their job duties while they are waiting to receive their TWIC cards. According to the TWIC proposed rule, it could take 30 to 60 days for TSA to perform background checks, produce the TWIC cards, and issue these cards to workers. TSA said that they are considering adding a provision to the proposed rule to allow workers temporary access to secure areas while they wait to receive their TWIC cards. Adding such a provision to the rule would address maritime industry concerns. According to TSA officials, the agency hopes to issue TWIC cards sooner than 30 days after a worker enrolls.

Potential Delays in Accessing Secure Areas

According to several industry stakeholders, the use of biometric card readers could disrupt the flow of commerce entering and exiting a port if each person or vehicle is not processed in a few seconds or if the readers experience technical problems. Specifically, if a worker or truck driver has problems with their fingerprint verification on a biometric card reader, they could create a long queue delaying several other workers and trucks waiting in line trying to enter secure areas of a port. According to the testing contractor's report, TWIC card readers rejected workers' access to secure areas in 4.8 percent of total access attempts during testing. These reject rates were comprised of two types. First, legitimate rejects were workers not allowed access to secure areas because they were not authorized to do so. Second, false rejects were workers not allowed to access secure areas although they were authorized to do so. According to TSA officials, the testing contractor did not determine what percentage of the total 4.8 percent reject rate was legitimate versus false rejects. In addition, neither the testing contractor's report nor TSA provided any information regarding wait times or delays experienced due to these reject rates at access control points during TWIC testing. The TWIC testing contractor attributed the cause of the reject rates during testing to transportation workers having rougher fingerprints than the average population, making it more difficult for card readers to verify their fingerprints. However, neither TSA nor the testing contractor developed solutions to the problem of reject rates that can be used during implementation of the TWIC program.

Several port officials we spoke with told us that delaying cargo entering and exiting a port could result in thousands of dollars lost by port terminal operators in the short term and millions in the long term. Stakeholders have suggested that TSA and the Coast Guard address concerns about delays by conducting additional testing of the TWIC program at a limited number of maritime facilities and vessels. Figure 4 shows a line of trucks transporting cargo into a large port facility through an access control point.

Figure 4: Trucks Carrying Cargo through an Access Control Point at a Large Maritime Facility

Source: Port of Los Angeles.

TSA and the Coast Guard officials stated that they recognize stakeholders' concerns regarding the potential impact of access control technology on the flow of commerce and, as a result, plan to obtain additional stakeholder input and comments as part of the second rulemaking to help address these concerns. We requested additional information from TSA on this rulemaking and how it would address concerns regarding the impact on commerce, however, TSA could not provide us any details.

Stringency of Background Checks

Industry stakeholders have stated that they generally support the TWIC program and its requirement that background checks be conducted on workers with unescorted access to secure areas to help ensure that these individuals do not pose a security threat. However, the stakeholders have also expressed some concern that certain disqualifying offenses may be too stringent and could lead to workers unnecessarily losing their jobs. For example, stakeholders stated that the disqualifying offenses should be terrorism related and not include lesser felonies currently in the TWIC proposed rule, such as fraud. In addition, stakeholders expressed concern that according to the TWIC proposed rule, being found guilty of certain

disqualifying criminal offenses, such as racketeering, will disqualify a person from receiving a TWIC card for their whole life, regardless of how long ago the worker committed the crime. The TWIC proposed rule would permit workers that do not pass the background check to appeal or request a waiver to obtain a TWIC card.[16]

Impact on Small Maritime Facilities and Vessels

Under the TWIC proposed rule, all Maritime Transportation Security Act (MTSA) regulated facilities and vessels would be required to use a TWIC card to control unescorted access to secure areas. Some industry stakeholders, however, disagree with applying uniform standards to all facilities and vessels in the maritime sector, regardless of size. Small facility and vessel officials providing comments on the TWIC proposed rule stated that if they are required to implement these requirements, they will have to conduct unnecessary checks of workers entering secure areas. For example, smaller vessels may have crews of less than 10 people, and checking TWIC cards each time a person enters a secure area is not necessary. In addition, stakeholders suggested that there should be flexibility in the final TWIC rule to exempt smaller facilities and vessels from requirements more applicable to large facilities and vessels. TSA and Coast Guard officials acknowledge the difficulties in applying the TWIC regulation to the entire maritime sector, and stated that they will obtain additional comments from stakeholders as part of the rulemaking process regarding the potential impact that the TWIC program could have on the flow of maritime commerce.

[16] Under TSA and the Coast Guard's TWIC proposed rule, an individual will be permanently disqualified from obtaining a TWIC card if he or she was ever convicted of or found not guilty by reason of insanity of any of the following crimes: murder; terrorism; espionage; sedition; treason; unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device; Racketeer Influenced and Corrupt Organizations (RICO) violations; a crime involving a transportation security incident; improper transportation of a hazardous material; and conspiracy or attempt to commit any of these crimes. Individuals convicted of or found not guilty by reason of insanity within the past 7 years, or released from prison within the past 5 years for any of the following crimes are disqualified from receiving a TWIC card: assault with intent to murder; kidnapping or hostage taking; rape or aggravated sexual abuse; extortion; robbery; arson; bribery; smuggling; immigration violations; racketeer influenced and corrupt organizations violations; distribution of, possession with intent to distribute, or importation of a controlled substance; dishonesty, fraud, or misrepresentation, including identity fraud; unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in firearms or other weapons; conspiracy; or attempt to commit any of these crimes. In addition, an applicant who is wanted or under indictment for a disqualifying felony is disqualified until the want or warrant is released.

Problems in Planning for and Overseeing the Contract to Test the TWIC Program

TSA experienced problems in planning for and overseeing the contract to test the TWIC program. Specifically, poor planning for the contract to test the TWIC program resulted in significant contract changes shortly after TSA awarded the contract, which contributed to a doubling of contract costs. According to TSA officials, delays in program development and pressure to begin TWIC testing caused the agency to award the contract before they had sufficient time to plan for and identify all of the requirements necessary to test the TWIC program in the initial contract. In addition, while the contract required testing certain key components of the TWIC program, TSA did not ensure that these key components were tested by the contractor. In addition to poor oversight, stakeholders told us that TSA did not effectively communicate and coordinate with them regarding any problems that arose during testing at their facility. TSA officials stated that the agency lacked adequate personnel to provide effective oversight of the contract to test the TWIC program and thus relied on the contractor to provide oversight of its own work and the work of its sub-contractors. Our previous reports have identified similar contract planning and oversight problems at TSA that led to increased contract costs. Specifically, in reports issued in 2004 and 2005, we found that both TSA and DHS contract policies did not adequately ensure that contract requirements and deliverables were clearly defined, and did not provide adequate oversight of contractor performance.[17] Since TSA will rely heavily on a private contractor to implement the TWIC program, it is important that comprehensive and clearly defined requirements are included in the implementation contract and contractor performance is closely monitored to help ensure effective and efficient accomplishment of contract purposes and to hold down costs.

Poor Planning by TSA in the Initial TWIC Testing Contract Contributed to a Doubling of Costs

TSA awarded the contract to test key components of the TWIC program in August 2004 for about $12 million. By the end of the testing phase, the total cost of the TWIC testing contract increased to over $27 million. According to the testing contractor, the cost increased because TSA added several key requirements that were necessary for testing the TWIC program to the contract after it was awarded. TSA officials confirmed that the addition of these key requirements caused the contract cost to increase.

[17] GAO, *Transportation Security Administration: High-Level Attention Needed to Strengthen Acquisition Function*, GAO-04-544 (Washington, D.C.: May 2004); and *Homeland Security: Successes and Challenges in DHS's Efforts to Create an Effective Acquisition Organization*, GAO-05-179 (Washington, D.C.: March 2005).

First, according to TSA and the testing contractor, although the initial contract did not stipulate a date to begin program testing, they initially agreed that the contractor should begin testing the TWIC program in April 2005. However, TSA officials moved up the start date to November 2004 to try to complete testing sooner. According to TSA and the testing contractor, the contractor incurred additional costs to move up the schedule. Second, TSA's initial testing contract was amended to require the contractor to install infrastructure necessary to test the TWIC program at transportation facilities. TSA added this requirement right after it awarded the contract because the agency learned that many testing facilities needed additional infrastructure to support testing the TWIC program and lacked the necessary funding to pay for it. According to TSA and the testing contractor, requiring the contractor to install infrastructure further increased the cost of the contract. Lastly, TSA changed the requirements after it awarded the testing contract to facilitate the enrollment of all port workers that were already enrolled in Florida's uniform port access credential program. This required the testing contractor to use a different approach to enrolling workers in Florida than was used at other TWIC testing locations. TSA did not include this approach in the original contract. According to TSA officials, these modifications were not included in the initial TWIC testing contract because TSA officials were under pressure to begin TWIC testing and did not have sufficient time to ensure that the contract included comprehensive and clearly defined requirements. TSA officials also stated that they knew they could modify the contract after it was awarded.

TSA is required to use the Federal Aviation Administration's (FAA) acquisition management system to guide government procurements, including contract planning and oversight, rather than the Federal Acquisition Regulation (FAR), which applies to most other federal agencies.[18] Although TSA is not subject to the requirements of the FAR, the FAR's requirements are designed to help ensure adequate contract planning. Specifically the FAR states that government personnel should avoid issuing contract requirements on an urgent basis, as was done during the TWIC testing contract, since this could increase contract prices. In addition, best practices for contract planning include defining key contract requirements and making critical decisions before moving forward and committing funds or resources to a major system, or

[18] ATSA directed TSA to adopt the FAA's acquisition management system. FAA, by law, is generally not subject to the requirements of federal acquisition laws and the FAR.

acquisition, such as the TWIC program. We have also previously reported that the development of any new system should follow a knowledge-based approach, including clearly defining system requirements through advanced planning, to achieve successful outcomes.[19] Adequate planning also includes making decisions before moving forward and taking action to prevent increases in cost, schedule delays, and degradations in performance and quality. Although contract requirements are often amended or added after initial contracts are awarded, the failure to consider and include critical requirements necessary to fully test the TWIC program and the resulting cost increases encountered is reflective of poor contract planning.

According to TSA, the agency is taking steps to address contract planning problems experienced during TWIC testing. Specifically, TSA officials told us that the TWIC program office has hired additional certified program managers and staff with technical expertise to assist in developing comprehensive and clearly defined requirements for the future contract to implement the TWIC program. However, it is not clear to what extent these actions will ensure that the contract to implement the TWIC program will include comprehensive and clearly defined contract requirements.

TSA Did Not Ensure That Key Components of the TWIC Program Were Tested

The TWIC testing contract required the contractor to test key components of the TWIC program and detect and resolve weaknesses identified during testing. TSA was responsible for ensuring that the contractor met all contract requirements. However, TSA did not effectively oversee the contractor's performance to ensure that key components of the program were tested. For example, the contractor was required to test the capability of the TWIC program to communicate information from a central database, such as TWIC cards that should be revoked if a worker is identified as a threat to security, to local facilities. However, TSA did not ensure that the contractor tested this capability. The independent contractor's assessment confirmed this component was not tested. The

[19] GAO, *Best Practices: Capturing Design and Manufacturing Knowledge Early Improves Acquisition Outcomes*, GAO-02-701 (Washington, D.C.: July 15, 2002). In a knowledge-based process, the achievement of each successive knowledge point builds on the preceding one, giving decision makers the knowledge they need—when they need it—to make decisions about whether to invest significant additional funds to move forward. Programs that follow a knowledge-based approach typically have a higher probability of successful cost and schedule outcomes.

assessment also found that the testing contractor did not fulfill 25 percent of the TWIC operational and performance contract requirements, such as the requirement that lost or stolen TWIC cards be revoked prior to issuing a new card. The independent assessment characterized the failure to meet this requirement during testing as a critical problem, as a terrorist could potentially use the lost or stolen card to access secure areas.

In addition, TSA officials did not perform certain tasks that are included in the agency's guidelines for contract oversight. TSA officials acknowledged that these functions were not performed because they lacked the oversight resources necessary to perform all of these tasks. For example, TSA officials acknowledged that the agency did not follow its contract oversight guidance in the following areas:

- **Performance and cost efficiency reporting.** A contracting officer technical representative (COTR) is a federal employee with technical knowledge of a specific program appointed by the contracting officer to ensure that contract requirements are met and to monitor the performance of the contractor. TSA's COTR guidelines state that one of the primary responsibilities of the COTR is to identify and report opportunities to improve contractor performance or cost efficiency to the contracting officer. However, according to TSA officials, no such performance reports were submitted by the COTR during the testing of the TWIC program.

- **Quality assurance planning.** The COTR guidelines require that the COTR follow a quality assurance plan for monitoring contractor performance. However, TSA officials stated that, although some limited monitoring and surveillance of the TWIC testing took place, they did not develop a quality assurance plan for the TWIC testing.

- **Evaluating contractor performance.** The COTR guidelines also state that the COTR is required to write their own evaluation of the contractor's technical performance. However, over 1 year after the completion of TWIC testing, TSA officials told us that an evaluation of the TWIC testing contractor's technical performance will be completed after the TWIC testing contractor completes transitional tasks.

According to TSA officials, the lack of TWIC program personnel as well as an over-reliance on the testing contractor to provide oversight of its own work and that of subcontractors caused inadequate oversight of the TWIC testing contract. The TWIC program office within TSA had seven individuals on staff and one person, the COTR, directly responsible for contract oversight. According to the COTR, more staff were needed to

provide adequate oversight of nearly 30 TWIC testing locations and multiple testing subcontractors. The COTR also stated that the TWIC testing contract was just one of several contracts that she was responsible for overseeing. As a result, the COTR visited only one location during TWIC program testing. According to TSA officials, the agency is taking steps to improve contract oversight practices. Specifically, TSA officials stated that the agency hired additional certified program managers, staff with technical expertise, and a new COTR to provide oversight of the future contract to implement the TWIC program. In addition, these officials told us that TSA has established a special office dedicated to managing TWIC contracts. However, until TSA develops its plans for monitoring contractor performance, it is not clear to what extent these actions will ensure that contractor performance and costs will be closely monitored.

In addition to oversight problems, stakeholders at all 15 TWIC testing locations we visited told us that TSA did not effectively communicate and coordinate with them regarding any problems that arose during testing at their facility. For example, at two maritime facilities we visited, officials told us that communication and coordination with TSA was the most significant problem they encountered during TWIC program testing. These officials stated that all communications from TSA and the testing contractor would stop for months during TWIC testing and that questions to TSA regarding the status of testing and various problems encountered often went unanswered. Another example of poor communication and coordination cited by stakeholders was that TSA never provided any results of the TWIC testing, including the final testing report, to the facilities that participated in the testing. According to TSA, the agency did not provide the final testing report to stakeholders because the report contained sensitive security information. Stakeholders stated that if TSA had an effective stakeholder feedback mechanism in place, TSA may have learned of testing problems and contractor performance issues sooner. In addition, an independent contractor's assessment of the TWIC testing also identified communication and coordination problems during their own site visits to 18 of the 28 TWIC testing locations. The independent contractor recommended that TSA develop procedures to provide more open and timely communication to stakeholders. TSA officials acknowledged that the agency could have better communicated with stakeholders at the TWIC testing locations.

We have previously highlighted the importance of effective communication and coordination between TSA and industry stakeholders to ensure that the agency is able to test and deliver programs that work

effectively. As a result, we recommended that TSA better communicate and coordinate with industry stakeholders and create a formal mechanism to ensure this communication and coordination takes place.[20] According to TSA officials, the agency recognizes that stakeholders involved in the TWIC testing should have been provided results of testing at their facilities and acknowledges that the agency did not establish a means of communicating and coordinating with stakeholders as part of the oversight process.

Another issue that arose during TWIC testing concerned TSA's decision to contract with the same company that was conducting the TWIC testing to provide the agency's TWIC program office management support, technical expertise, and assistance in providing contract oversight. The program management contractor staff worked in TSA's TWIC program office and helped evaluate contract deliverables submitted by its own company, such as the final report summarizing the results and conclusions of the TWIC testing. Although TSA said that the two contracts involved separate teams from the same company, conflict of interest concerns in this particular situation were such that TSA required the contractor to address organizational conflict of interest concerns in a mitigation plan and paid an independent contractor to review the TWIC testing.[21]

Further, the independent assessment contractor found that there were problems with the testing contractor's report, such as inaccurate and missing information. The assessment also stated that TSA did not adequately (1) define testing contract requirements, (2) develop a comprehensive implementation plan to secure adequate stakeholder involvement, or (3) monitor TWIC program schedules and costs. As a result, the independent assessment recommended that the contractor's

[20] GAO, *Maritime Security*: *Enhancements Made, but Implementation and Sustainability Remain Key Challenges*, GAO-05-448T (Washington, D.C.: May, 17 2005); and *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington, D.C.: September 2005).

[21] TSA Acquisition Management System (AMS) provisions set out, in pertinent part, that it is TSA policy to avoid contracting with contractors who have unreasonable organizational conflicts of interest. Actual or perceived organizational conflict of interest situations, under the AMS provisions, may be addressed through a mitigation plan. TSA AMS § 3.1.7-3. The TSA's AMS derives from the Aviation and Transportation Security Act (ATSA) of 2001, which exempts TSA from the Federal Acquisition Regulation and most federal acquisition laws, and instead directed the TSA to adopt the Federal Aviation Administration's (FAA) acquisition management system while also authorizing TSA to modify the application of the FAA's acquisition management system to TSA as appropriate. 49 U.S.C. § 114 (o).

final report not be relied upon when making decisions about the implementation of TWIC until these problems were corrected.

In previous reports, we identified problems with TSA's contracts and contractor oversight practices, including contracts without clearly defined requirements and inadequate oversight that caused initial TSA contract costs to increase.[22] We have also reported on TSA and DHS's lack of policies that provide clear guidance on defining contract requirements or contract oversight.[23] For example, the report notes that clearly defining requirements allows more precise cost estimates for specific contracts as well as better approximations of the timelines for completion. In addition, inadequate oversight increases the risk that costs will increase in a labor hour and cost reimbursement contract as used here.

Conclusions

The TWIC program was established in response to congressional direction to mitigate the threat of terrorists and other unauthorized persons from accessing the nation's ports and other transportation facilities. The maritime industry and other transportation stakeholders are generally supportive of the TWIC program as a means to strengthen access control security and establish a national standard for worker identification credentials. TSA tested the TWIC program at a select number of transportation facilities to identify problems, develop solutions to these problems, and help determine how TWIC can be effectively implemented across the nation. However, the TWIC testing fell short of meeting its goals. Specifically, during testing, TSA issued cards to only about 1,700 workers and tested card readers at 19 facilities, a much smaller population than planned, and TSA did not fully test all key components of the TWIC program, such as biometric card readers. As a result, TSA faces the challenge of transitioning from this limited testing to successful implementation of the program on a much larger scale covering 750,000 workers at over 3,500 maritime facilities and 10,800 vessels. While TSA has taken some actions to address problems identified during TWIC program testing, the agency and the maritime industry still face key challenges in ensuring that the program will meet its intended goal of

[22] GAO, *Transportation Security Administration: High-Level Attention Needed to Strengthen Acquisition Function*, GAO-04-544 (Washington, D.C.: May 2004).

[23] GAO, *Homeland Security: Successes and Challenges in DHS's Efforts to Create an Effective Acquisition Organization*, GAO-05-179 (Washington, D.C.: March 2005).

providing an effective means of preventing unauthorized access to secure areas.

TSA has recently announced that it will use two separate rulemakings to implement the TWIC program. The first will provide the requirements for enrolling workers, conducting background checks, and issuing TWIC cards. A subsequent rule will include requirements for purchasing and installing TWIC access control technologies. Postponing the issuance of requirements for TWIC access control technologies will afford the maritime industry additional time to comment on these requirements. However, it is not clear what, if any, additional testing of the TWIC access control technologies will be conducted as part of this subsequent rulemaking to ensure that they work effectively. Moreover, TSA's decision to issue two TWIC rules poses an additional challenge in that TSA will need to ensure that the TWIC cards issued to workers enrolled under the first rule will be compatible with the card reader technologies that will be part of the second rule. TSA's decision to rapidly move forward with implementation of the TWIC program without developing and testing solutions to identified problems could lead to additional problems, increased costs, and further program delays without achieving the program's intended goals. Considering the large investment that the federal government and maritime industry will be required to make to implement the TWIC program, it is particularly important that solutions to the problems and challenges facing the program be developed and tested before implementation to avoid wasting resources. We have found during prior work that in a rush to implement programs quickly, TSA has not always followed a disciplined development process, including conducting appropriate systems testing, and did not always follow their own systems development guidance when developing programs. As a result, they experienced program delays and cost overruns, and lacked assurance that the programs would meet their intended goals.

TSA's lack of contract planning, oversight, and communication and coordination with stakeholders during testing of the TWIC program, and past contract planning and oversight problems, raise questions about whether TSA can ensure that the contract to implement the TWIC program will include comprehensive and clearly defined requirements or that the agency will provide adequate oversight of contractor performance. TSA officials stated that the agency has taken steps to address these problems by hiring additional staff with technical and program management expertise to assist in developing contract requirements and providing oversight. While these actions may address problems that occurred during TWIC program testing, whether they will resolve all of the contract

planning and oversight problems will not be clear until TSA develops and awards the contract to implement the TWIC program and develops plans for overseeing and evaluating contractor performance and communicating and coordinating with maritime industry stakeholders.

Recommendations for Executive Action

To help ensure that the TWIC program can be implemented as efficiently and effectively as possible, we recommend that the Secretary of Homeland Security direct the Assistant Secretary of Homeland Security for the Transportation Security Administration, in close coordination with the Commandant of the U.S. Coast Guard, to take the following two actions:

1. Before TWIC is implemented in the maritime sector, develop and test solutions to the problems identified during TWIC program testing, and raised by stakeholders in commenting on the TWIC proposed rule, to ensure that all key components of the TWIC program work effectively. In developing and testing these solutions, TSA should:

    - ensure that the TWIC program will be able to efficiently enroll and issue TWIC cards to large numbers of workers;
    - ensure that the technology necessary to operate the TWIC program will be readily available to industry stakeholders and will function effectively in the maritime sector, including biometric card readers and the capability to link facility access control systems with the national TWIC database;
    - ensure that the TWIC program balances the added security it provides with the potential effect that the program could have on the flow of maritime commerce; and
    - closely coordinate with maritime industry stakeholders—particularly those that are currently implementing or using biometric access control systems—to learn from their experiences.

2. Strengthen contract planning and oversight practices before awarding the contract to implement the TWIC program to achieve the following purposes:

    - ensure that the contract to implement the TWIC program contains comprehensive and clearly defined requirements;
    - ensure that resources are available and measures are in place to provide effective government oversight of the contractor's performance; and
    - establish a communication and coordination plan to capture and address the views and concerns of maritime industry stakeholders during implementation.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. On September 22, 2006, we received written comments on the draft report, which are reproduced in full in appendix II. DHS concurred with the findings and recommendations and stated that the report will help improve TSA's management of the TWIC program and strengthen oversight of contractor performance. DHS further stated that the report's recommendations will help facilitate the nationwide implementation of the TWIC card and thus, the agency has already taken steps to implement them.

Regarding our recommendation to develop and test solutions to the problems identified during TWIC program testing, and raised by stakeholders in commenting on the TWIC proposed rule, DHS stated that it is taking a number of actions. Specifically, to ensure that the TWIC program will be able to efficiently enroll and issue TWIC cards to large numbers of workers, TSA is using experience gained during TWIC testing to improve the enrollment and card issuance process, which should address the problems encountered during testing. For example, TSA plans to use an easier and faster form of scanning to capture workers' fingerprints and is taking additional steps to ensure that the process for enrolling workers and issuing TWIC cards is efficient. In addition, according to DHS, TSA is seeking an experienced and capable contractor to enroll workers and operate the information technology systems necessary to support the program. Taking these steps should help TSA to address the problems experienced during testing regarding enrollment and card issuance. Nevertheless, TSA will face the challenge of enrolling and issuing TWIC cards to a significantly larger population of workers than was enrolled during testing.

Concerning our recommendation that DHS ensure that the technology necessary to operate the TWIC program will be readily available to industry stakeholders and will function effectively in the maritime sector, including biometric card readers and the capability to link facility access control systems with the national TWIC database, DHS stated that TSA and the Coast Guard will not require maritime facilities and vessels to purchase or install card readers as part of the first rulemaking process. Instead, requirements for biometric card readers and access control technologies will be part of a subsequent rulemaking. According to DHS, the two-phased rulemaking process allows more time for maritime facility and vessels owners and operators to plan for the installation of biometric card readers and access control infrastructure and allows the public additional opportunity to comment on this aspect of the program. In addition, TSA is considering additional field testing of biometric card

readers within the funding and schedule parameters of the TWIC program and has already solicited stakeholders' involvement in these tests. Furthermore, according to DHS, the General Services Administration (GSA) and NIST are currently testing products, including biometric card readers, for compliance with FIPS 201 standards. GSA is also developing a list of qualified access control technology products and vendors that will be available for purchase by maritime facilities and vessels to implement the TWIC program in the future. Obtaining additional comments from the public regarding TWIC access control technology requirements, conducting additional testing of TWIC program technologies in the maritime environment, and ensuring that access control technologies are compliant with FIPS 201 standards are important steps for ensuring that the TWIC program works effectively in the maritime environment. In regard to linking facility access control systems with the national TWIC database, DHS stated that facilities and vessels will be provided secure web access to a list of TWIC cards that are lost, stolen, expired, or belong to individuals found to pose a threat to security.

In addressing our recommendation that TSA and the Coast Guard ensure that the TWIC program balances the added security it provides with the potential effect that the program could have on the flow of maritime commerce, DHS stated that TSA and the Coast Guard have reviewed industry comments, are cognizant of stakeholder concerns, and acknowledge the potential impact that the TWIC program could have on the flow of maritime commerce. As a result, TSA and Coast Guard plan to obtain additional comments on this issue from industry stakeholders in the second rulemaking pertaining to access control technology. Soliciting additional comments from maritime industry stakeholders should help TSA and the Coast Guard balance the added security of the TWIC program with the potential affects on the flow of maritime commerce. Conducting additional testing of TWIC in the maritime environment would further help TSA and the Coast Guard determine how to balance security and the flow of maritime commerce.

With regard to our recommendation that DHS closely coordinate with maritime industry stakeholders—particularly those that are currently implementing or using biometric access control systems—to learn from their experiences, DHS stated that the TWIC program is considering field testing of biometric card reader technology to support the second phase of the TWIC program within the funding and schedule parameters of the program. According to DHS, multiple TWIC stakeholders have expressed an interest in participating in this field testing. In addition, TSA and the Coast Guard plan an upcoming conference of TWIC qualified contractors

and TWIC stakeholders to discuss experiences during TWIC testing. DHS also stated that the agency has invited other stakeholders to provide feedback on the TWIC program. Taking action to better coordinate with maritime stakeholders are steps in the right direction and will be essential to effectively implementing the TWIC program.

In response to our recommendation that TSA strengthen contract planning and oversight practices before awarding the contract to implement the TWIC program, DHS stated that it is taking several actions to implement this recommendation. Specifically, to ensure that the contract to implement the TWIC program contains comprehensive and clearly defined requirements, TSA has recently selected qualified contractors and released the request for proposal (RFP) to implement the TWIC program. The TWIC RFP includes a detailed requirements document that identifies the performance outcomes expected to be met by the contractor selected to implement the TWIC program. According to DHS, any future changes to the TWIC requirements will be managed under a formal change control process. If properly implemented, these actions should better position TSA to ensure that the TWIC implementation contract contains comprehensive and clearly defined requirements.

Regarding our recommendation that TSA ensure that resources are available and measures are in place to provide effective government oversight of the contractor's performance, DHS stated that the TWIC program has recently established a Program Control Office to help oversee contractor performance and deliverables. In addition, the TWIC program has developed a Quality Assurance and Surveillance Plan and acceptable quality levels of performance in the TWIC RFP to provide a foundation for contract management and oversight. TSA has also hired additional staff to provide better program management and improved oversight of TWIC contracts. Allocating additional resources and taking steps to ensure that TSA provides effective oversight of the TWIC implementation contract are important steps toward improving contract oversight. If properly implemented, these actions should address the intent of this recommendation.

Concerning our recommendation that TSA establish a communication and coordination plan to capture and address the views and concerns of maritime industry stakeholders during implementation, DHS stated that the TWIC program has increased its communication and coordination efforts with stakeholders during the TWIC rulemaking process and plans to continue these activities during implementation of the program. According to DHS, the TWIC program office has developed a

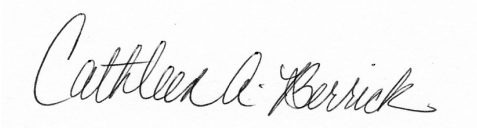
communication strategy and plan and the TWIC RFP requires the TWIC implementation contractor to establish a communications plan to provide information to stakeholders and address their concerns during implementation. Developing plans to better communicate and coordinate with stakeholders will be key to the success of the TWIC program.

DHS also offered technical comments and clarifications, which we have considered and incorporated where appropriate.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 21 days after its issue date. At that time, we will provide copies of this report to the Secretary of Homeland Security, Assistant Secretary of the Transportation Security Administration, Commandant of the U.S. Coast Guard, and other interested congressional committees as appropriate. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or you staff have any questions about this report, please contact me at (202) 512-3404 or at berrickc@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 III.

Sincerely yours,



Cathleen A. Berrick
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to answer the following questions: (1) What problems, if any, did testing of the TWIC program identify and what challenges, if any, do DHS and industry stakeholders face in implementing the program? and (2) To what extent, if at all, did TSA experience problems in planning for and overseeing the contract to test the TWIC program?

To address our first objective, to identify the problems, if any, during testing of the TWIC program and the challenges, if any, DHS and industry stakeholders face in implementing the program, we interviewed TSA and Coast Guard officials regarding the development of the TWIC program, results of TWIC program testing, and challenges identified with implementing the program. To determine the status of the TWIC program, goals, and requirements of TWIC testing and testing results, we obtained and analyzed TWIC program documents, including program management plans, the final report on TWIC testing, an independent contractor's assessment of TWIC testing, the TWIC proposed rule, and the TWIC regulatory impact analysis. We also reviewed applicable laws, regulations, policies, and procedures to determine the requirements for implementing the TWIC program. We attended public meetings held by TSA and the Coast Guard in Newark, New Jersey; Tampa, Florida; and Long Beach, California; to obtain industry comments on the TWIC proposed rule. We also reviewed stakeholder comments submitted to TSA and the Coast Guard during the rulemaking process. We conducted site visits to 15 of the 28 facilities that participated in testing the TWIC program in California, Delaware, Florida, New Jersey, New York, and Pennsylvania to obtain information on stakeholder experiences regarding the TWIC testing, observe the operation of the TWIC program at these facilities, and discuss any challenges associated with implementing TWIC. We visited testing facilities in each of the three testing regions—East Coast, West Coast, and Florida—as well as locations representing the maritime, aviation, and rail modes of transportation. We selected the 15 facilities based on geographic location, mode of transportation, and diversity of facility size and area of business operations. Table 3 lists the 15 facilities we visited that participated in TWIC testing.

Table 3: Facilities We Visited that Participated in the TWIC Testing

Facility	Location
East Coast Region	
Amtrak Operations Center	Wilmington, Delaware
Gloucester Terminals, LLC	Camden, New Jersey
Maritime Exchange	Philadelphia, Pennsylvania
Port of Wilmington	Wilmington, Delaware
Macarthur Airport	Islip, New York
West Coast Region	
Port of Los Angeles	Los Angeles, California
Port of Long Beach	Long Beach, California
American Present Lines	Los Angeles, California
APM Terminal, Inc.	Los Angeles, California
Long Beach Container Terminal, Inc.	Long Beach, California
British Petroleum	Long Beach, California
Los Angeles International Airport	Los Angeles, California
Florida Region	
Port Everglades	Fort Lauderdale, Florida
Port of Palm Beach	Palm Beach, Florida
Port of Pensacola	Pensacola, Florida

Source: GAO.

To address our second objective, to determine to what extent, if at all, the contract to test the TWIC program identified contract planning and oversight problems that should be addressed before implementing the program, we interviewed TSA officials regarding the planning for and oversight of the contract to test the TWIC program. We obtained and analyzed TWIC program documents, including the TWIC testing contract and report, an independent contractor's assessment of TWIC testing, and TSA's internal contract planning and oversight guidance. We interviewed TWIC contractor officials regarding contract requirements, testing results, and TSA's planning for and oversight of the testing contract. We also interviewed officials from the independent contractor that assessed the TWIC testing to discuss the results of this assessment. Further, we reviewed the methodology of the independent contractor's assessment by examining documents, interviewing contractor officials, and performing internal analyses to help ensure data reliability. Our work was also informed by our prior reports and testimony related to TWIC, maritime and transportation security, and TSA and DHS contracting practices.

We conducted our work from August 2005 through September 2006 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

September 22, 2006

Ms. Cathleen A. Berrick
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on draft report GAO-06-982, "DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program." The Department of Homeland Security (DHS) concurs with the recommendations and appreciates GAO's work in planning, conducting, and issuing this study. The findings in this report will help improve TSA's management of the Transportation Worker Identification Credential (TWIC) program and strengthen oversight of contract performance. TSA believes these recommendations will help facilitate the nationwide implementation of a common TWIC system for increased security throughout the Nation, and thus has already taken steps to implement GAO's recommendations.

TSA developed the TWIC program, beginning in December 2001, to review, identify, and mitigate security deficiencies to ensure that only properly cleared and authorized personnel could gain access to secure areas of the Nation's transportation system. The mission of the TWIC program is to develop a common security threat assessment and credential or standard for transportation workers requiring unescorted physical and logical access to secure areas of the national transportation system. In achieving the TWIC program's mission, three overarching goals must be achieved: improved security, enhanced commerce, and the protection of privacy. A plan was devised in early 2002 to develop the TWIC in four phases: Phase I – Planning, Phase II -- Technical Evaluation, Phase III – Prototype and Phase IV-- Production. The TWIC Prototype phase was completed on June 30, 2005.

TSA is using the testing experience to make improvements to the enrollment and card issuance process. For example, TSA plans to use an easier and faster form of scanning to capture workers' fingerprints. Moreover, we are taking additional steps to ensure that the process for enrolling workers and issuing TWIC cards is efficient.

www.dhs.gov

TSA and Coast Guard published a Notice of Proposed Rulemaking (NPRM) on May 22, 2006, and held a series of public meetings in Newark, NJ; Tampa, FL; St. Louis, MO; and Long Beach, CA, to gather comments on the proposed rule. The public commenting period in the proposed rule for TWIC closed on July 6, 2006. TSA and Coast Guard received over 1,900 comments to the NPRM. Many of these comments voiced concern regarding card and reader technology, analysis of economic impact, potential negative impacts to commerce, and uncertainty as to how TWIC requirements for facilities and vessels could be met. After a review of the comments received on the NPRM and the requests for extension, TSA and the Coast Guard decided that facility and vessel owners and operators will not be required to purchase or install card readers during the first phase of the TWIC implementation. Additionally, a requirement to purchase and install card readers will not be implemented until the public is afforded further opportunity to comment on that aspect of the TWIC program.

TSA recently issued a request for proposals from private contractors interested and capable of implementing the TWIC program and maintaining the information technology systems that support the program. Eight companies were selected as qualified vendors and their responses are expected by October 2, 2006. TSA plans to award the implementation contract by December 2006 for the maritime sector and expects to provide additional guidance when TWIC is applied to other modes.

TSA has added new team members to the TWIC program to augment the existing team with the critical skills required to implement TWIC, including technology and systems integration, acquisition, contract management, program management, and deployment. The new personnel have enabled the TWIC team to provide better direction to the overall program and to improve oversight of TWIC contracts. The blend of new team members and personnel with institutional knowledge of the prototype system is providing improvements to the management structure for the overall program. The TWIC program has also established a Program Control Office to manage TWIC financials, contractor performance, and deliverables.

The program is in the final planning stages for nationwide implementation and is focused on lessons learned from the Prototype phase to further refine requirements. TSA is also assessing system enhancements that would enhance consistency with Homeland Security Presidential Directive 12 and its technical standard, Federal Information Processing Standard 201-1. TSA anticipates publication of the Final Rule by the end of the 2006 calendar year. The findings from the prototype effort along with GAO's input are being used to finalize the implementation and management approach for nationwide TWIC implementation.

Our specific approaches to all of the GAO recommendations are reflected below.

Recommendation 1: Before TWIC is implemented in the maritime sector, develop and test solutions to the problems identified during TWIC program testing, and raised by stakeholders in commenting on the TWIC proposed rule, to ensure that all key components of the TWIC system work effectively. In developing and testing these solutions, TSA should:

a) Ensure that the TWIC program will be able to efficiently enroll and issue TWIC cards to large numbers of workers;

Concur. The TWIC program prototype demonstrated the ability to efficiently enroll workers and issue credentials. TSA plans to build upon the experiences from the prototype and acquire the services of a contractor to enroll the large number of workers expected to participate in the TWIC program. TSA recently published a "request for qualifications" seeking firms that are appropriately experienced and interested in enrolling workers in the TWIC program and to operate and maintain the information technology systems that support the program. Eight companies were selected as qualified vendors. The TWIC Request for Proposal (RFP) was released to these qualified vendors on September 1, 2006, with a response date of October 2, 2006. TSA expects to award the contract by December 2006.

b) Ensure that the technology necessary to operate the TWIC program will be readily available to industry stakeholders and will function effectively in the maritime sector, including biometric card readers and the capability to link facility access control systems with the national TWIC database;

Concur. TSA and Coast Guard published a Notice of Proposed Rulemaking (NPRM) on May 22, 2006, and held a series of public meetings in Newark, NJ; Tampa, FL; St. Louis, MO; and Long Beach, CA, to gather comments on the proposed rule. TSA and Coast Guard received over 1,900 comments to the NPRM. Many of these comments voiced concern regarding card and reader technology, analysis of economic impact, potential negative impacts to commerce, and uncertainty as to how TWIC requirements for facilities and vessels could be met.

After a review of the comments received during the comment period and requests for extension, TSA and the Coast Guard have concluded that facility and vessel owners and operators will not be required to purchase or install card readers during the first phase of the TWIC implementation. Additionally, a requirement to purchase and install card readers will not be implemented until the public is afforded further opportunity to comment on that aspect of the TWIC program. The details of this approach will be explained in the next rulemaking. The two-phased rulemaking process allows more time for port facility and vessel owners and operators to plan for installation of biometric readers and access control infrastructure and allows additional opportunity for public comment on access control requirements and biometric reader standards. Having taken into consideration the concerns of many stakeholders regarding biometric readers in harsh maritime environments, TSA and the Coast Guard are designing the TWIC program to be consistent with Homeland Security Presidential Directive 12 and its technical standard, the Federal Information Processing Standard (FIPS) 201-1, which establishes a common policy and technical standards for a common identification standard for Federal Employees and Contractors. The General Services Administration (GSA) and the National Institute of Standards and Technology (NIST) are currently testing products, including biometric readers, for compliance with FIPS 201-1. The GSA's FIPS 201-1 Approved Products List identifies qualified products and vendors which have met the certification and testing standards established by both NIST and GSA. There is no requirement to design the TWIC process to comply with FIPS-201-1, but consistency with the standard has many benefits. Alignment with the FIPS 201-1 technology standard enhances the likelihood that many products and services will be available for use in the TWIC program. The 'chain of trust' and privacy protections built into the standard also are critical to the integrity of the program.

The capability to link facility access control systems within the national TWIC database is expected to be accomplished by providing port facility and vessel owners and operators with secure web access to the TWIC revocation list, which identifies credentials that are no longer valid. The revocation list includes the unique card identifiers of lost, stolen, or expired TWICs, as well as the TWICs of individuals who are found to be a security risk through the vetting process. This allows owners and operators flexibility in determining and implementing their specific technology requirements and supports the decentralized model that is critical in the maritime environment.

c) Ensure that the TWIC program balances the added security it provides with the potential effect that the program could have on the flow of maritime commerce;

Concur. Many of the comments on the May 22, 2006, NPRM were concerns regarding card and reader technology, analysis of economic impact, potential negative impacts to commerce, and uncertainty as to how TWIC requirements for facilities and vessels could be met. TSA has weighed these comments along with the security benefits TWIC will provide.

TSA and the Coast Guard have reviewed industry comments, are cognizant of stakeholder concerns, and acknowledge the potential impact that the TWIC program could have on the flow of maritime commerce. As a result, TSA and the Coast Guard plan to obtain additional comments on this issue from industry stakeholders in the second rulemaking pertaining to access control technology.

d) Closely coordinate with maritime industry stakeholders – particularly those that are currently implementing or using biometric access control systems – to learn from their experiences.

Concur. Multiple TWIC stakeholders have expressed an interest in participating in field testing of biometric reader technology in cooperation with TSA and Coast Guard. The TWIC program is exploring field testing of biometric reader technology to support the second phase of the TWIC program within the funding and schedule parameters of the program.

A recent example of ongoing coordination includes a meeting among TSA, the Coast Guard and the Port of Wilmington on August 29, 2006, to discuss TWIC program status and to request their support in hosting the TWIC qualified vendors during the upcoming TWIC Bidder's Conference and to discuss their experience with the TWIC prototype. Other stakeholders have also been invited to provide feedback.

Recommendation 2: Strengthen contract planning and oversight practices before awarding the contract to implement the TWIC program to achieve the following:

a) Ensure that the contract to implement the TWIC program contains comprehensive and clearly defined requirements;

Concur. TSA recently published a "request for qualifications" seeking firms that are appropriately experienced and interested to enroll workers in the TWIC program and to operate

and maintain the information technology systems that support the program. Eight companies were selected as qualified vendors. The TWIC Request for Proposal (RFP) was released to these qualified vendors on September 1, 2006. Proposals are due October 2, 2006, and contract award is expected before the end of calendar year 2006. The TWIC RFP includes a detailed requirements document that identifies the performance outcomes expected to be met by the contractor in operating and maintaining the TWIC system. Any future changes to the TWIC system requirements will be managed under a formal change control process.

b) Ensure that resources are available and measures are in place to provide effective government oversight of the contractor's performance;

Concur. The TWIC program has established a Program Control Office to manage TWIC financials, contractor performance, and deliverables. The program has included a Quality Assurance Surveillance Plan and Acceptable Quality Levels (AQLs) of performance in the TWIC RFP to provide the foundation and capability for strong contract management and oversight. Additionally, the TWIC program office added staff to augment the existing team with the critical skills required to effectively manage TWIC, including technology and systems integration, acquisition, contract management, deployment, and program management. The new personnel have enabled the team to provide better direction to the overall program and to improve oversight of TWIC contracts. The blend of new personnel and personnel with historical knowledge of the prototype system provides an improved management structure for the overall program.

c) Establish a communication and coordination plan to capture and address views and concerns of maritime industry stakeholders during implementation.

Concur. The TWIC program has coordinated outreach, communication, and coordination efforts throughout the TWIC rulemaking process and plans to continue these activities during nationwide implementation.

During the TWIC rulemaking process, TSA and Coast Guard held a series of public meetings in Newark, NJ; Tampa, FL; St. Louis, MO; and Long Beach, CA, to gather comments on the proposed rule. During the NPRM analysis phase, TSA and Coast Guard met with additional industry stakeholders who requested meetings to listen to concerns about TWIC implementation; these meetings are summarized in the docket for the TWIC NPRM.

In addition, TSA and Coast Guard recently met with the Port of Wilmington on August 29, 2006, to discuss TWIC program status and to request their support in hosting the TWIC qualified vendors during the upcoming TWIC Bidder's Conference and to discuss their experience with the TWIC prototype.

The program office has developed a Communication Strategy and Plan that addresses the need to communicate with TWIC stakeholders, including port facility and vessel owners and operators, potential TWIC applicants, TWIC holders, unions, industry associations, other interested parties, Captains of the Port, and other Government entities. The TWIC RFP also requires the

enrollment contractor to establish a communications plan to address stakeholder and user communications and change management issues throughout the initial enrollment process.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgements

GAO Contact

Cathleen A. Berrick (202) 512-3404

Acknowledgements

In addition to the contact above, John Hansen, Assistant Director, Chris Currie, Nicholas Larson, Michele Mackin, Geoff Hamilton, Katherine Davis, Chuck Bausell, Michele Fejfar, Richard Hung, and Pille Anvelt 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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548