GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

April 13, 2011

The Honorable John D. Rockefeller, IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

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

Subject: *Transportation Worker Identification Credential: Mailing Credentials to Applicants' Residences Would Not Be Consistent with DHS Policy*

Securing transportation systems and facilities requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and necessary for supporting international commerce. As we have previously reported, these systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.[1]

To help enhance the security of these systems and facilities, the Maritime Transportation Security Act of 2002 (MTSA) required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they both possess a biometric transportation security card and are authorized to be in such an

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

area.[2] MTSA further tasked the Secretary with the responsibility to issue biometric transportation security cards to eligible individuals unless the Secretary determines that an applicant poses a security risk warranting denial of the card. The Transportation Worker Identification Credential (TWIC) program is designed to implement these biometric maritime security card requirements. The program requires maritime workers to undergo a background check to obtain a biometric identification card. This card is required for an individual to be eligible for unescorted access to secure areas of vessels and facilities. It is still the responsibility of facility and vessel owners to determine who should be granted access to their facilities or vessels.

Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) and the United States Coast Guard are responsible for implementing and enforcing the TWIC program. TSA's responsibilities include enrolling TWIC applicants, conducting background checks to assess individuals' potential security threat, and issuing TWICs. In January 2007, TSA contracted out TWIC enrollment center operations to enroll applicants and issue TWICs to approved applicants. This contract expires in June 2012. The Coast Guard is responsible for developing TWIC-related security regulations and ensuring that MTSA-regulated maritime facilities and vessels are in compliance with these regulations. In addition, DHS's Screening Coordination Office (SCO) facilitates coordination among the various DHS components involved in TWIC, such as TSA and the Coast Guard, as well as the United States Citizenship and Immigration Services (USCIS), which, through an interagency agreement, personalizes the credentials and ships them to enrollment centers, and the Federal Emergency Management Agency, which administers grant funds in support of the TWIC program.[3]

Section 818(b)(1) of the Coast Guard Authorization Act of 2010[4] provides that the Comptroller General shall submit a report to the House Committee on Homeland Security and the Senate Committee on Commerce, Science, and Transportation assessing the costs, technical feasibility, and security measures associated with procedures to (1) deliver a transportation security card (i.e., a TWIC) to an approved applicant's place of residence in a secure manner or (2) allow an approved applicant to receive the card at an enrollment center of the individual's choosing. To meet the mandate, we analyzed the factors affecting DHS's ability to mail cards to an enrollment center of choice or an approved applicant's residence, and the security and cost implications DHS reports are associated with such actions.

---

[2] Pub. L. No. 107-295, 116 Stat. 2064 (2002). Under United States Coast Guard regulations, a secure area, in general, is an area over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard–approved security plan. For most maritime facilities, the secure area is generally any place inside the outermost access control point. For a vessel or outer continental shelf facility, such as off-shore petroleum or gas production facilities, the secure area is generally the whole vessel or facility. Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

[3] DHS established its Screening Coordination Office (SCO) to coordinate and harmonize the numerous and disparate credentialing and screening initiatives within DHS. A card is personalized when the cardholder's personal information, such as photograph and name, are added to the card.

[4] Pub. L. No. 111-281, 124 Stat. 2905, 3000 (2010).

To assess the factors affecting DHS's ability to mail cards to an approved applicant's residence or enrollment center of choice, we reviewed existing processes for TWIC production, personalization, activation, and issuance. We analyzed documentation provided by TSA regarding TWIC program systems and processes, such as the TWIC *User Manual for Trusted Agents*, concept of operations, and statement of work. We also reviewed information provided by USCIS on its credential production and personalization process, such as information on the Secure Mail Initiative.[5] We interviewed TSA and USCIS officials about the feasibility of mailing cards to an applicant's residence or enrollment center of choice. We also interviewed relevant officials from the TSA TWIC contractor to discuss the possibility of modifying the current TWIC card production and mailing processes.

To identify the security implications associated with mailing cards to an individual's residence or enrollment center of choice, we analyzed pertinent regulations, policies, and guidance establishing requirements for secure issuance of credentials.[6] We interviewed officials from TSA and SCO to identify how security requirements were identified for the TWIC processes and obtain views on how changes to the TWIC activation and issuance process might affect security. We interviewed officials from USCIS to obtain information about their approach to securely mailing other government credentials to individual residences. We also interviewed officials from the Department of Commerce's National Institute of Standards and Technology (NIST) to confirm our understanding of Federal Information Processing Standards (FIPS) Publication 201-1 requirements and security standards, and officials from the Coast Guard to identify what impact the mailing of TWICs might have on compliance and enforcement.

To determine costs DHS has associated with mailing cards to an applicant's residence or enrollment center of choice, we analyzed TWIC program fee requirements as established in the TWIC rule and supporting regulatory evaluation to understand the costs related to the current activation and issuance process, and how changes to the issuance process could influence program fees. We also reviewed GAO's *Cost Estimating and Assessment Guide* and DHS's *Cost Benefit Analysis Guidebook* to determine the required elements for estimating costs and DHS requirements for conducting a cost-benefit analysis.[7] We interviewed officials from TSA and USCIS about the cost implications of mailing cards to an applicant's residence or enrollment center of choice.

Our work for this report was also informed by ongoing work we are conducting for your committees and others evaluating the extent to which TWIC program controls

---

[5] USCIS's Secure Mail Initiative utilizes the United States Postal Service's Priority Mail with Delivery Confirmation service to enhance accountability and customer service in the delivery of secure immigration documents to customers. This initiative allows USCIS to prove when secure documents were mailed, and allows customers to track their documents through the mailing process.

[6] See, for example, Federal Information Processing Standards (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (Gaithersburg, Md., March 2006), and National Institute of Standards and Technology Special Publication 800-63, *Electronic Authentication Guideline* (Gaithersburg, Md., April 2006).

[7] See GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009), and Department of Homeland Security, C*ost Benefit Analysis Guidebook*, *Version 2.0* (Washington D.C., February 2006).

provide reasonable assurance that unescorted access to secure areas of MTSA-regulated facilities and vessels is limited to those possessing a legitimately issued TWIC and who are authorized to be in such an area.[8] We expect to issue a report with the final results from this review later this year.

We conducted this performance audit from February 2011 to April 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Starting in February 2009, TSA allowed applicants to designate an enrollment center of their choosing where a TWIC would be activated and issued. However, several factors limit the ability of DHS to mail TWICs to an approved applicant's residence. For example, it would not meet current or proposed NIST guidelines for credential issuance (FIPS 201-1) that require a biometric match be performed before providing the card to the applicant. Such a match must be done in person using information either from the TWIC or the enrollment record. DHS and TSA made a policy decision to align the TWIC program with these guidelines because it used the latest technology, secured critical facilities with the same processes used by federal agencies, and would allow interoperability in an emergency. Should DHS and TSA change their policy that the TWIC program be aligned with FIPS 201-1, TSA and USCIS, the organization that personalizes TWICs for TSA, stated that changes could be made to existing business processes and systems to accommodate such a change but that this would require significant changes to the existing systems and processes used to produce and issue cards. Regarding the cost implications of mailing TWICs to residences, specific program requirements to accomplish this goal would need to be identified before an accurate cost estimate can be made.

Background

TWIC History and Purpose

In November 2001, the Aviation and Transportation Security Act (ATSA) was enacted, requiring TSA, among other things, to work with airport operators to strengthen access control points in secured areas and to consider using biometric access control systems, or similar technologies, to verify the identities of individuals who seek to enter a secure airport area.[9] In response to ATSA, TSA established the TWIC program in December 2001.[10] In November 2002, MTSA was enacted and required the

[8] The committees that requested the work include the Senate Committee on Commerce, Science, and Transportation, including the Subcommittee on Oceans, Atmosphere, Fisheries, and Coast Guard and the Subcommittee on Surface Transportation and Merchant Marine Infrastructure, Safety, and Security; the House Committee on Transportation and Infrastructure, including the Subcommittee on Coast Guard and Maritime Transportation; and the House Committee on Homeland Security.
[9] Pub. L. No. 107-71, 115 Stat. 597 (2001).
[10] TSA was transferred from the Department of Transportation to DHS pursuant to requirements in the Homeland Security Act, enacted on November 25, 2002 (Pub. L. No. 107-296, 116 Stat. 2135 (2002)).

Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics to control access to secure areas of maritime transportation facilities and vessels.[11] In addition, the Security and Accountability For Every Port Act of 2006 amended MTSA and directed the Secretary of Homeland Security, among other things, to implement the TWIC pilot project to test TWIC use with biometric card readers.[12] Once the pilot has concluded, a report on the findings of the pilot is expected to inform the development of a card reader rule on how TWIC will be implemented with biometric card readers. DHS currently estimates that a notice of proposed rulemaking will be issued late in 2011 and that the final rule will be promulgated no earlier than the end of 2012.

In January 2007, a federal regulation (known as the TWIC credential rule) set a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker seeking unescorted access to secure areas of MTSA-regulated facilities and vessels must possess a TWIC.[13] Currently, TWICs are primarily used as visual identity cards—or flash passes—where a card is to be visually inspected before a cardholder enters a secure area of a MTSA-regulated port or facility. As of March 24, 2011, TSA reported over 1.8 million enrollments and 1.7 million card activations.[14]

Current TWIC Enrollment, Card Production, Activation, and Issuance Processes

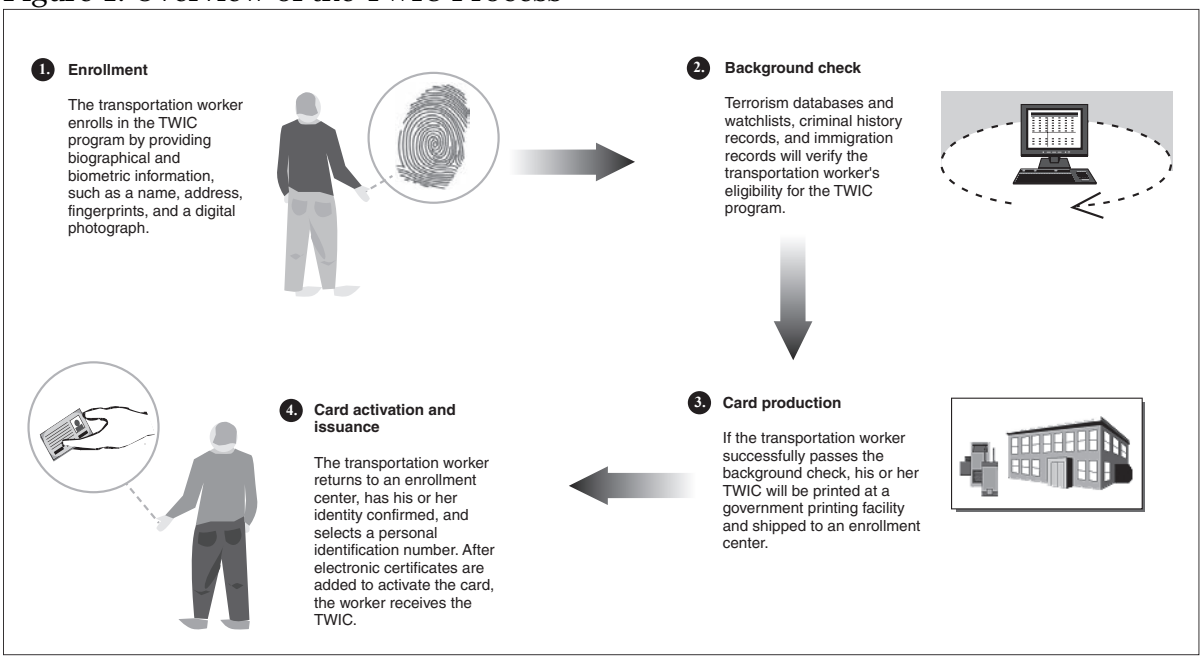
In January 2007, TSA hired a contractor for the TWIC program. The contractor was charged with establishing enrollment centers, enrolling applicants, and activating applicants' TWICs once applicants successfully passed security threat assessments (background checks).[15] During the enrollment process, transportation workers are to pay an enrollment fee of up to $132.50;[16] provide biographic information, such as their name, date of birth, and address; and are to be photographed and fingerprinted by trusted agents at the enrollment centers.[17] Trusted agents are subcontractors who have been authorized by the federal government to enroll transportation workers in the TWIC program and issue TWICs. After TSA determines that a worker has passed

[11] Prior to TWIC, facilities and vessels administered their own approaches for controlling access based on the perceived risk at the facility. These approaches, among others, included requiring people seeking access to have a reason for entering, facility-specific identification, and in some cases, a background check. Some ports and port facilities still maintain their own credentials.
[12] Pub. L. No. 109-347, 120 Stat. 1884 (2006).
[13] 72 Fed. Reg. 3492 (2007).
[14] Prior to issuing a TWIC, each TWIC is activated, or turned on, after the person being issued the TWIC provides a personal identification number (PIN).
[15] TSA is to conduct a security threat assessment of each TWIC applicant. TWIC program threat assessment processes include conducting a background check to determine whether each TWIC applicant is a security risk to the United States. These checks, in general, can include checking criminal history records, immigration status, terrorism databases and watch lists, and records indicating an adjudication of lack of mental capacity, among other things. TSA regulations define "security threat" to mean an individual whom TSA determines or suspects of posing a threat to national security, to transportation security, or of terrorism.
[16] The fee for a TWIC is $132.50 and is valid for 5 years. Workers with current, comparable background checks will pay a reduced fee of $105.25. If workers are eligible to pay the lower price, their TWICs will expire 5 years from the date of the comparable credential. The cost of a replacement TWIC, if the original is lost, stolen, or damaged, is $60.00.
[17] Under TSA's contract for the TWIC program, the contractor is responsible for staffing enrollment centers with trained trusted agents.

the background check, the worker's information is to be provided to the USCIS-operated federal card production facility in Corbin, Kentucky, where TWICs are to be personalized with applicants' information, such as an applicant's photograph and name. After this step is completed, the card is to be sent to the appropriate enrollment center for activation and issuance to the applicant. TWICs remain active for 5 years. Under the current process, at the end of 5 years, cardholders must apply for a new card and pay an additional fee.[18]

Once a worker's TWIC is personalized, the worker is to be notified and must return to an enrollment center in person to obtain and activate his or her card. To activate a card, a trusted agent is to confirm an individual's identity by reviewing the individual's government-issued photo identification and matching his or her live fingerprint to the biometric template stored on the card. The worker is to select a personal identification number (PIN), which is used to protect the digital information on the card (i.e., electronic certificates for applicant identity, digital signing, digital encryption, and card authorization).[19] The worker is to reenter his or her PIN to accept and agree to TWIC holder responsibilities and confirm that certain electronic TWIC features are working. Once the PIN is reentered, the TWIC is to be issued to the worker for use in accessing MTSA-regulated facilities and vessels. Figure 1 contains an overview of the TWIC process.

Figure 1: Overview of the TWIC Process



Source: GAO analysis of TSA information.

[18] On March 15, 2011, H.R. 1105 was introduced in the House of Representatives with provisions designed to ensure that TWICs held by certain maritime workers do not expire until DHS issues the final reader rule or December 31, 2014, whichever is earlier.

[19] This PIN allows for two-factor authentication of the TWIC holder's identity by confirming something the person has (the TWIC) and something the person knows (the PIN). Further, MTSA-regulated facilities and vessels may require TWIC users to use the PIN to unlock electronic information in a TWIC, such as the TWIC holder's picture.

Mailing TWICs to Approved Applicants' Residences Would Not Be Consistent with DHS Policy and Has Security and Cost Implications

Applicants Can Pick Up TWICs at the Enrollment Center of Their Choice

At the program's inception, TSA required TWIC applicants to return to the same enrollment center where they enrolled to activate and pick up their TWICs. However, according to TSA officials, starting in February 2009, TSA allowed applicants to designate an enrollment center of their choosing where the TWIC would be activated and issued.[20] The agency spent $187,000 modifying the program to allow activation and issuance at enrollment centers of applicants' choosing.[21] According to TSA, the procedure was changed to improve customer service by allowing applicants more flexibility in obtaining a TWIC. In addition, this change required revisions to the TWIC information technology system (TWIC system) and operational procedures for enrollment, which were addressed through a contract modification and related task order with the contractor.

Mailing TWICs to Approved Applicants' Residences Would Not Be Consistent with Current DHS and TSA Policy

Existing DHS and TSA policy does not allow a TWIC to be mailed to an approved applicant's residence. Under current policy, an applicant must be physically present to pick up a card. On August 27, 2004, the President issued Homeland Security Presidential Directive 12 (HSPD-12) mandating the establishment of a standard for identification of federal employees and contractors. HSPD-12 requires the use of a common identification card for access to federally controlled facilities[22] and information systems to help enhance security, increase efficiency, and reduce security fraud, among other benefits. In response to HSPD-12, NIST issued the Federal Information Processing Standards Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, in February 2005 and updated it in March 2006 (FIPS 201-1).[23] The overall goal of FIPS 201-1 is to achieve appropriate security assurance for individuals seeking physical access to federally controlled government facilities and electronic access to government information systems. Although not required to comply with FIPS 201-1, as a policy

[20] According to TSA officials, beginning in February 2009, individuals could call the TWIC Help Desk to request that their TWICs be sent to an alternate enrollment center for activation and issuance. In May 2009, TSA added an option where, at the time of enrollment, individuals could indicate that they would like to pick up their TWICs from sites other than those at which they enrolled.

[21] TSA has spent an additional $230,000 transferring workers' cards to alternate enrollment centers for activation and issuance.

[22] Office of Management and Budget implementation guidance on HSPD-12, in general, defines "federally controlled facilities" to mean (1) federally owned buildings or leased space, all or any portion of which is under the jurisdiction, custody, or control of a department or agency covered by the directive; (2) federally controlled commercial space shared with nongovernmental tenants (for example, if a department or agency leased the 10th floor of a commercial building, the directive applies to the 10th floor only; (3) government-owned, contractor-operated facilities; and (4) facilities under a management and operating contract, such as for the operation, maintenance, or support of a government-owned or government-controlled research, development, special production, or testing establishment.

[23] FIPS 201-1 is currently undergoing a mandatory 5-year review. For the purposes of this review, we used the current draft version issued by NIST, which was dated March 2011. This is commonly referred to as the March 2011 draft FIPS 201-2.

decision, DHS and TSA decided to align the TWIC program with these standards where possible, even though the focus of the standard is not maritime facilities or vessels and TWIC holders are not limited to federal employees and contractors. TSA noted in the 2006 TWIC Notice of Proposed Rulemaking that there were benefits to designing the TWIC program in alignment with FIPS 201-1, including avoiding obsolescence by using the latest technology, securing critical facilities with the same process used by federal agencies, and having interoperability during an emergency.

FIPS 201-1 is currently being revised and, according to a NIST official, is expected to be superseded by updated guidance in 2012. According to NIST officials, both the current FIPS 201-1 and the March 2011 draft FIPS 201-2 require an applicant to be physically present to pick up a card. Specifically, the current FIPS 201-1 and March 2011 draft FIPS 201-2 require that prior to the delivery of the newly issued personal identity verification card to an applicant, the issuer perform a biometric match of the applicant against the biometric included in the card or in the enrollment record. Upon successful match, the card is released to the applicant. According to NIST officials, this requirement means that the applicant must be present to receive the card since this match must be done when the card is released to the user. They also noted that the requirement for an applicant to be physically present during card issuance is consistent with the control objective of the current and March 2011 draft FIPS 201-2 that the cards should only be issued to individuals whose true identity has been verified and that having the individual present when the card is issued is key to accomplishing this objective.

If DHS and TSA were to change the current policy of remaining aligned with FIPS 201-1 card issuance requirements, according to an USCIS official, it would be possible for USCIS to mail personalized TWICs directly from the Corbin, Kentucky, facility to individual residences. For example, beginning December 7, 2010, USCIS used its Secure Mail Initiative to mail nearly 900,000 permanent residence cards and employment authorization documents to individual residences. The Secure Mail Initiative uses U.S. Priority Mail shipping with delivery confirmation to ensure that the credentials are delivered to the desired recipient. USCIS officials also stated that they are willing to work with TSA to personalize and distribute TWICs to individual residences, to enrollment centers, or to both, if TSA requests that they do so.

However, according to TSA officials, mailing TWICs to individual residences rather than enrollment centers would be possible but would require significant and potentially costly changes to TWIC systems, processes, regulations, and contracts. TSA officials stated that these changes would include modifications to the software that operates the enrollment center workstations and the technology systems used to collect, store, and transfer TWIC applicant biographic and biometric information among the various components involved in enrollment, background checks, card personalization, and card activation and issuance. As TWICs are currently shipped in batches from the USCIS facility in Corbin, Kentucky, to approximately 135 enrollment centers, TSA officials said TSA would have to establish processes and procedures to manage cards that are undeliverable because of incorrect or changed addresses. According to program officials, the TWIC program has had thousands of pieces of correspondence (for example, notices of threat assessment results and requests for additional information) returned as undeliverable, as the maritime transportation population is very mobile. TSA officials said that an additional complication would be

that TSA would also need to integrate the revised TWIC system with other components, such as the automated notification system and the Web site that provides card status. TSA officials also said that such changes to the established TWIC processes would require comprehensive testing prior to implementation. For example, before the TWIC program began operations in 2007, TSA went through a technical evaluation period, which began in 2003, and a 2-year prototype period (2004-2005) during which the current processes were established, tested, and modified. TSA believes that a similar effort would be required before implementing a major business process reengineering to allow for mailing TWICs to individuals.

TSA officials also said that making this change to the TWIC program might also require regulatory changes to the portions of the January 2007 TWIC credential rule pertaining to the activation and issuance of the TWICs. The TWIC credential rule identifies TWIC program requirements and fees for use of TWIC as a flash pass. TWIC program officials also noted that the time required to modify the credential rule would be influenced by several other regulations currently under development such as a proposed rule on using TWICs with biometric card readers.

According to TSA officials, mailing TWICs directly to individual residences would require changes to TSA's program management contract along with the interagency agreement for card personalization with USCIS. The contract and agreement reflect the existing approach to TWIC enrollment, activation, and issuance. TSA officials said they would have to execute modifications to the TWIC contract and to an interagency agreement with USCIS for card personalization services. TSA officials stated that this would require a major effort from the TWIC program and acquisitions staff that would include defining requirements, preparing statements of work, reviewing contractor deliverables, negotiating changes and executing the modifications, and monitoring the work.

In addition to TSA and DHS's policy to align the TWIC program with FIPS 201-1 standards, TSA and Coast Guard officials expressed other security concerns related to mailing TWICs to individual residences. TSA officials stated that mailing TWICs to approximately 1.7 million addresses would increase the chances of having a large number of lost and unaccounted for cards. As TWICs are currently only required to be used as a flash pass, if TWICs were lost in the mail, delivered to incorrect addresses, or stolen from mailboxes, then those cards could be used by individuals who did not undergo a background check to attempt to obtain unescorted access to secure areas of a MTSA-regulated facility. Both TSA and Coast Guard officials responsible for the TWIC program stressed a need to ensure that an authentic TWIC—activated or unactivated—did not end up in the wrong person's hands if the credential is not issued in person.

Accurate Cost Estimates for Mailing Cards to Residences Cannot Be Made without First Identifying Specific Program Requirements

As we reported in March 2009, high-quality cost estimates, when developed, generally include defining program characteristics, such as technology implications, security needs and risk items, as well as staff requirements.[24] According to TSA officials,

[24] GAO-09-3SP.

because they do not believe that mailing TWICs to individual residences is advisable from a security standpoint—the change would not allow the TWIC program to remain aligned with FIPS 201-1—they have not invested resources in developing a cost estimate. TSA officials further stated that if DHS directed TSA to deviate from the FIPS 201-1 standard to allow for an alternative issuance process, the TWIC program would first need to assess whether it is feasible by comparing the cost of making this change with the potential security risk associated with redesigning the current FIPS 201-1–aligned system.

While TSA officials have not developed a specific cost estimate, they anticipate that it could be costly to reengineer the TWIC production, personalization, delivery, and activation processes to mail individual TWICs directly to transportation workers. Costs would include changes to the TWIC enrollment and issuance processes, the TWIC system, and processes for mailing the cards. According to TSA, these necessary changes could result in an increase in the fee that transportation workers currently pay to obtain their TWICs (currently set at a maximum of $132.50). According to these officials, because the TWIC program is required by statute to pay for program costs through user fees,[25] if TSA were to modify the scope of the program, TSA would need to change the TWIC rule and fees to reflect the modification. TSA estimates that changes to the TWIC credential rule could take up to 24 months to execute because the agency would have to issue and solicit comments on both a proposed and final rule.

According to procurement officials at TSA, if the agency were to allow TWICs to be mailed to applicants' residences, these changes would be incorporated as a modification to the next TWIC contract, which will be awarded before the current contract expires in June 2012. According to TSA, it has no plans to modify the current contract to allow mailing of TWICs to transportation workers' residences.

Agency Comments and Our Evaluation

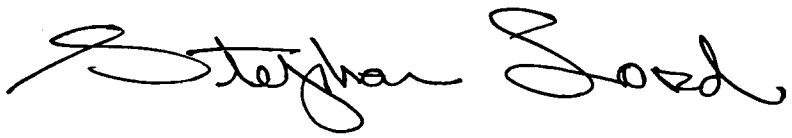
We requested comments on a draft of this report from the Secretary of Homeland Security. DHS did not provide written comments to include in the report. However, on April 7, 2011, TSA's TWIC Program Manager and USCIS's Integrated Document Production Branch Business Operations Specialist provided oral technical comments, which we incorporated as appropriate. Additionally, in e-mails received on April 7, 2011 and April 8, 2011, respectively, the TSA and USCIS audit liaisons provided technical comments, which we incorporated as appropriate.

- - - - -

We are sending copies of this report to the Secretary of Homeland Security, appropriate congressional committees, and other interested parties. This report also is available at no charge on the GAO Web site at http://www.gao.gov.

[25] 6 U.S.C. § 469(a).

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



Stephen M. Lord
Director, Homeland Security and Justice Issues

Enclosure

Enclosure I: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, David Bruno, Assistant Director; Geoffrey Hamilton; Richard Hung; John C. Martin; Lara Miklozek; Julie E. Silvers; and Michelle R. Su made key contributions to this report.

(440952)