United States Government Accountability Office

Testimony

Before the Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. EST
Thursday, May 9, 2013

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Card Reader Pilot Results Are Unreliable; Security Benefits Should Be Reassessed

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

Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee:

I am pleased to be here today to discuss our work examining the Department of Homeland Security's (DHS) Transportation Worker Identification Credential (TWIC) program. Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have serious consequences. Maritime workers, including longshoremen, mechanics, truck drivers, and merchant mariners, access secure areas of the nation's estimated 16,400 maritime-related transportation facilities and vessels, such as cargo container and cruise ship terminals, each day while performing their jobs.[1]

The TWIC program is intended to provide a tamper-resistant biometric credential[2] to maritime workers who require unescorted access to secure areas of facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA).[3] TWIC is to enhance the ability of MTSA-regulated facility and vessel owners and operators to control access to their facilities and verify workers' identities. Under current statute and regulation, maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities or vessels are required to obtain a TWIC,[4] and facility and vessel operators are required by regulation to visually inspect each worker's TWIC before granting unescorted access.[5] Prior to being granted a TWIC, maritime workers are

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

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

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

[4]46 U.S.C. § 70105(a); 33 C.F.R. § 101.514.

[5]33 C.F.R. §§ 104.265(c), 105.255(c).

required to undergo a background check, known as a security threat assessment.

Within DHS, the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) jointly administer the TWIC program. USCG is leading efforts to develop a new TWIC regulation (rule) regarding the use of TWIC cards with readers (known as the TWIC card reader rule). The TWIC card reader rule is expected to define if and under what circumstances facility and vessel owners and operators are to use electronic card readers to verify that a TWIC card is valid. To help inform this rulemaking and to fulfill the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) requirement,[6] TSA conducted a TWIC reader pilot from August 2008 through May 2011 to test a variety of biometric readers, as well as the credential authentication and validation process. The TWIC reader pilot, implemented with the voluntary participation of maritime port, facility, and vessel operators, was to test the technology, business processes, and operational impacts of deploying card readers at maritime facilities and vessels prior to issuing a final rule.[7] Among other things, the SAFE Port Act required that DHS submit a report on the findings of the pilot program to Congress.[8] DHS submitted its report to Congress on the findings of the TWIC reader pilot on February 27, 2012.[9] The Coast Guard Authorization Act of 2010 required that, among other things, GAO conduct an assessment of the report's findings and recommendations.[10]

We have been reporting on TWIC progress and challenges since September 2003.[11] Among other issues, we highlighted steps that TSA

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

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

[8]46 U.S.C. § 70105(k)(4).

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

[10]Pub. L. No. 111-281, § 802, 124 Stat. 2905, 2989.

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

and USCG were taking to meet an expected surge in initial enrollment as well as various challenges experienced in the TWIC testing conducted by a contractor for TSA and USCG from August 2004 through June 2005. We also identified challenges related to ensuring that the TWIC technology works effectively in the harsh maritime environment.[12] In November 2009, we reported on the design and approach of a pilot initiated in August 2008 to test TWIC readers, and found that DHS did not have a sound evaluation methodology to ensure information collected through the TWIC reader pilot would be complete and accurate.[13] Moreover, in May 2011, we reported that internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals.[14]

My statement today highlights the key findings of a report we released yesterday on the TWIC program that addressed the extent to which the results from the TWIC reader pilot were sufficiently complete, accurate, and reliable for informing Congress and the TWIC card reader rule.[15] For the report, among other things, we assessed the methods used to collect and analyze pilot data since the inception of the pilot in August 2008. We analyzed and compared the pilot data with the TWIC reader pilot report submitted to Congress to determine whether the findings in the report are based on sufficiently complete, accurate, and reliable data. Additionally, we interviewed officials at DHS, TSA, and USCG with responsibilities for overseeing the TWIC program, as well as pilot officials responsible for coordinating pilot efforts with TSA and the independent test agent

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

[13]*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).

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

[15]GAO, *Transportation Worker Identity Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198 (Washington, D.C.: May 8, 2013).

(responsible for planning, evaluating, and reporting on all test events), about TWIC reader pilot testing approaches, results, and challenges. Our investigators also conducted limited covert testing of TWIC program internal controls for acquiring and using TWIC cards at four maritime ports to update our understanding of the effectiveness of TWIC at enhancing maritime security since we reported on these issues in May 2011. Our May 2013 report includes additional details on our scope and methodology. We conducted this work in accordance with generally accepted government auditing standards, and conducted the related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

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

Our review of the pilot test identified several challenges related to pilot planning, data collection, and reporting, which affected the completeness, accuracy, and reliability of the results.

Pilot Planning

DHS did not correct planning shortfalls that we identified in our November 2009 report.[16] We determined that these weaknesses presented a challenge in ensuring that the pilot would yield information needed to inform Congress and the card reader rule and recommended that DHS components implementing the pilot—TSA and USCG—develop an evaluation plan to guide the remainder of the pilot and identify how it would compensate for areas where the TWIC reader pilot would not provide the information needed. DHS agreed with the recommendations; however, while TSA developed a data analysis plan, TSA and USCG reported that they did not develop an evaluation plan with an evaluation methodology or performance standards, as we recommended. The data analysis plan was a positive step because it identified specific data

[16]GAO-10-43.

elements to be captured from the pilot for comparison across pilot sites. If accurate data had been collected, adherence to the data analysis plan could have helped yield valid results. However, TSA and the independent test agent[17] did not utilize the data analysis plan. According to officials from the independent test agent, they started to use the data analysis plan but stopped using the plan because they were experiencing difficulty in collecting the required data and TSA directed them to change the reporting approach. TSA officials stated that they directed the independent test agent to change its collection and reporting approach because of TSA's inability to require or control data collection to the extent required to execute the plan.

Data Collection

We identified eight areas where TWIC reader pilot data collection, supporting documentation, and recording weaknesses affected the completeness, accuracy, and reliability of the pilot data

1. **Installed TWIC readers and access control systems could not collect required data on TWIC reader use, and TSA and the independent test agent did not employ effective compensating data collection measures.** The TWIC reader pilot test and evaluation master plan recognizes that in some cases, readers or related access control systems at pilot sites may not collect the required test data, potentially requiring additional resources, such as on-site personnel, to monitor and log TWIC card reader use issues. Moreover, such instances were to be addressed as part of the test planning. However, the independent test agent reported challenges in sufficiently documenting reader and system errors. For example, the independent test agent reported that the logs from the TWIC readers and related access control systems were not detailed enough to determine the reason for errors, such as biometric match failure, an expired TWIC card, or that the TWIC was identified as being on the list of revoked credentials. The independent test agent further reported that the inability to determine the reason for errors limited its ability to understand why readers were failing, and thus it was unable to determine whether errors encountered were due to TWIC cards, readers, or users, or some combination thereof.

[17]To conduct the TWIC reader pilot, TSA contracted with the Navy's Space and Naval Warfare Systems Command (SPAWAR) to serve as the independent test agent to plan, analyze, evaluate, and report on all test events.

2. **Reported transaction data did not match underlying documentation.** A total of 34 pilot site reports were issued by the independent test agent. According to TSA, the pilot site reports were used as the basis for DHS's report to Congress. We separately requested copies of the 34 pilot site reports from both TSA and the independent test agent. In comparing the reports provided, we found that 31 of the 34 pilot site reports provided to us by TSA did not contain the same information as those provided by the independent test agent. Differences for 27 of the 31 pilot site reports pertained to how pilot site data were characterized, such as the baseline throughput time used to compare against throughput times observed during two phases of testing. However, at two pilot sites, Brownsville and Staten Island Ferry, transaction data reported by the independent test agent did not match the data included in TSA's reports. Moreover, data in the pilot site reports did not always match data collected by the independent test agent during the pilot.

3. **Pilot documentation did not contain complete TWIC reader and access control system characteristics.** Pilot documentation did not always identify which TWIC readers or which interface (e.g., contact or contactless interface) the reader used to communicate with the TWIC card during data collection.[18] For example, at one pilot site, two different readers were tested. However, the pilot site report did not identify which data were collected using which reader.

4. **TSA and the independent test agent did not record clear baseline data for comparing operational performance at access points with TWIC readers.** Baseline data, which were to be collected prior to piloting the use of TWIC with readers, were to be a measure of throughput time, that is, the time required to inspect a TWIC card and complete access-related processes prior to granting entry. However, it is unclear from the documentation whether acquired data were sufficient to reliably identify throughput times at truck, other vehicle, and pedestrian access points, which may vary.

5. **TSA and the independent test agent did not collect complete data on malfunctioning TWIC cards.** TSA officials observed malfunctioning TWIC cards during the pilot, largely because of broken antennas. If a TWIC with a broken antenna was presented for a

[18]As used in this statement, "contactless mode" refers to the use of TWIC readers for reading TWIC cards without requiring that a TWIC card be inserted into or make physical contact with a TWIC reader.

contactless read, the reader would not identify that a TWIC had been presented, as the broken antenna would not communicate TWIC information to a contactless reader. In such instances, the reader would not log that an access attempt had been made and failed.

6. **Pilot participants did not document instances of denied access.** Incomplete data resulted from challenges documenting how to manage individuals with a denied TWIC across pilot sites. Specifically, TSA and the independent test agent did not require pilot participants to document when individuals were granted access based on a visual inspection of the TWIC, or deny the individual access as may be required under future regulation. This is contrary to the TWIC reader pilot test and evaluation master plan, which calls for documenting the number of entrants "rejected" with the TWIC card reader system operational as part of assessing the economic impact. Without such documentation, the pilot sites were not completely measuring the operational impact of using TWIC with readers.
7. **TSA and the independent test agent did not collect consistent data on the operational impact of using TWIC cards with readers.** TWIC reader pilot testing scenarios included having each individual present his or her TWIC for verification; however, it is unclear whether this actually occurred in practice. For example, at one pilot site, officials noted that during testing, approximately 1 in 10 individuals was required to have his or her TWIC checked while entering the facility because of concerns about causing a traffic backup. Despite noted deviations in test protocols, the reports for these pilot sites do not note that these deviations occurred. Noting deviations in each pilot site report would have provided important perspective by identifying the limitations of the data collected at the pilot site and providing context when comparing the pilot site data with data from other pilot sites.
8. **Pilot site records did not contain complete information about installed TWIC readers' and access control systems' design.** TSA and the independent test agent tested the TWIC readers at each pilot site to ensure they worked before individuals began presenting their TWIC cards to the readers during the pilot. However, the data gathered during the testing were incomplete. For example, 10 of 15 sites tested readers for which no record of system design characteristics were recorded. In addition, pilot reader information was identified for 4 pilot sites but did not identify the specific readers or associated software tested.

According to TSA, a variety of challenges prevented TSA and the independent test agent from collecting pilot data in a complete and

consistent fashion. Among the challenges noted by TSA, (1) pilot participation was voluntary, which allowed pilot sites to stop participation at any time or not adhere to established testing and data collection protocols; (2) the independent test agent did not correctly and completely collect and record pilot data; (3) systems in place during the pilot did not record all required data, including information on failed TWIC card reads and the reasons for the failure; and (4) prior to pilot testing, officials did not expect to confront problems with nonfunctioning TWIC cards. Additionally, TSA noted that it lacked the authority to compel pilot sites to collect data in a way that would have been in compliance with federal standards. In addition to these challenges, the independent test agent identified the lack of a database to track and analyze all pilot data in a consistent manner as an additional challenge to data collection and reporting. The independent test agent, however, noted that all data collection plans and resulting data representation were ultimately approved by TSA and USCG.

Reporting

As required by the SAFE Port Act and the Coast Guard Authorization Act of 2010, DHS's report to Congress on the TWIC reader pilot presented several findings with respect to technical and operational aspects of implementing TWIC technologies in the maritime environment. However, DHS's reported findings were not always supported by the pilot data, or were based on incomplete or unreliable data, thus limiting the report's usefulness in informing Congress about the results of the TWIC reader pilot. For example, reported entry times into facilities were not based on data collected at pilot sites as intended. Further, the report concluded that TWIC cards and readers provide a critical layer of port security, but data were not collected to support this conclusion.

Because of the number of concerns that we identified with the TWIC pilot, in our March 13, 2013, draft report to DHS, we recommended that DHS not use the pilot data to inform the upcoming TWIC card reader rule. However, after receiving the draft that we sent to DHS for comment, on March 22, 2013, USCG published the TWIC card reader notice of proposed rulemaking (NPRM), which included results from the TWIC card reader pilot.[19] We subsequently removed the recommendation from our final report, given that USCG had moved forward with issuing the NPRM

[19]78 Fed. Reg. 17,782 (Mar. 22, 2013).

and had incorporated the pilot results into the proposed rulemaking. In its official comments on our report, DHS asserted that some of the perceived data anomalies we cited were not significant to the conclusions TSA reached during the pilot and that the pilot report was only one of multiple sources of information available to USCG in drafting the TWIC reader NPRM. We recognize that USCG had multiple sources of information available to it when drafting the proposed rule; however, the pilot was used as an important basis for informing the development of the NPRM, and the issues and concerns that we identified remain valid.

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

Chairman Mica, Ranking Member Connolly, and members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Steve Lord 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 statement. Individuals making key contributions to this statement include Dave Bruno, Assistant Director; Joseph P. Cruz; and James Lawson. Key contributors for the previous work that this testimony is based on are listed within each individual product.