OFFICE OF INSPECTOR GENERAL

Review of Coast Guard's Oversight of the TWIC Program

Homeland Security

September 28, 2018

OIG-18-88

DHS OIG Highlights

Review of Coast Guard's Oversight of the TWIC Program

September 28, 2018

Why We Did This Audit

We determined the extent to which the Department of Homeland Security completed an assessment of the security value of the Transportation Worker Identification Credential (TWIC) program as required by Public Law 114–278, Section 1(b). We also determined the extent to which the United States Coast Guard's (Coast Guard) oversight of the TWIC program ensures only eligible individuals are granted unescorted access to secure areas of regulated facilities.

What We Recommend

We made four recommendations aimed at improving the Department's oversight of the TWIC program.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

DHS did not complete an assessment of the security value of the TWIC program as required by Public Law 114–278, Section 1(b). This occurred because DHS experienced challenges identifying an office responsible for the effort. As a result, the Coast Guard does not have a full understanding of the extent to which the TWIC program addresses security risks in the maritime environment. This will continue to impact the Coast Guard's ability to properly develop and enforce regulations governing the TWIC program. For example, the Coast Guard did not clearly define the applicability of facilities that have certain dangerous cargo in bulk when developing a final rule to implement the use of TWIC readers at high-risk maritime facilities. Without oversight and policy improvements in the TWIC program, high-risk facilities may continue to operate without enhanced security measures, putting these facilities at an increased security risk.

The Coast Guard needs to improve its oversight of the TWIC program to reduce the risk of transportation security incidents. Due to technical problems and lack of awareness of procedures, the Coast Guard did not make full use of the TWIC card's biometric features as intended by Congress to ensure only eligible individuals have unescorted access to secure areas of regulated facilities. During inspections at regulated facilities from fiscal years 2016 through 2017, the Coast Guard only used electronic readers to verify, on average, about 1 in every 15 TWIC cards against the Transportation Security Administration's canceled card list. This occurred because the majority of the TWIC readers in the field have reached the end of their service life. Furthermore, the Coast Guard's guidance governing oversight of the TWIC program is fragmented, which led to confusion and inconsistent inspection procedures. This resulted in fewer regulatory confiscations of TWIC cards.

Management Response

The Department concurred with all four recommendations and described the corrective actions it is taking and plans to take.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 28, 2018

MEMORANDUM FOR: William N. Bryan
Senior Official Performing the
Duties of the Under Secretary
Science and Technology

Rear Admiral John P. Nadeau
Assistant Commandant for Prevention Policy
United States Coast Guard

FROM: Sondra F. McCauley
Acting Assistant Inspector General for Audits

SUBJECT: *Review of Coast Guard's Oversight of the TWIC Program*

For your action is our final report, *Review of Coast Guard's Oversight of the TWIC Program*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving oversight of the TWIC program. The Department of Homeland Security concurred with all four recommendations. Based on information provided in your response to the draft report, we consider the four recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions at (202) 981-6000, or your staff may contact Maureen Duddy, Deputy Assistant Inspector General for Audits, at (617) 565-8723.

Background

Ports, waterways, and vessels handle billions of dollars in cargo annually. Ports are susceptible to terrorist attacks because of their size, general proximity to metropolitan areas, volume of cargo being processed, and link to the global supply chain. 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.

After the September 11th terrorist attacks, the *Maritime Transportation Security Act of 2002* (MTSA) (Public Law 107–295) required the Department of Homeland Security to prescribe certain regulations preventing individuals from having unescorted access to secure[1] areas of MTSA-regulated facilities. To meet this requirement, DHS initiated the Transportation Worker Identification Credential (TWIC) program to help protect critical portions of the Nation's maritime transportation infrastructure from acts of terrorism. Key requirements include:

- All individuals[2] who need unescorted access to secure areas of MTSA-regulated facilities must present a biometric[3] TWIC card and have a valid business case for requesting access.
- All individuals who do not hold a TWIC card, but are otherwise authorized to be in the secure area, must be escorted by another individual who holds a valid TWIC.
- Prior to being granted a TWIC card, the individuals must successfully complete a background check, known as a security threat assessment. The assessment includes vetting the individuals against terrorist-, crime-, and immigration-related databases.

Within DHS, the Transportation Security Administration (TSA) and United States Coast Guard (Coast Guard) jointly administer the TWIC program:

- TSA conducts background checks and recurrent vetting, issues credentials, and takes civil enforcement action against individuals engaged in credential alteration and fraudulent use.
- In the maritime environment, the Coast Guard develops and enforces TWIC regulations, takes civil action against facility owners, and refers criminal matters against facility owners and cardholders to the appropriate Federal, state, or local prosecuting agency.

[1] A secure area is an area that has security measures for access control.
[2] Federal officials and law enforcement officials at the state or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas of MTSA-regulated facilities.
[3] A biometric card contains an encrypted file with the cardholder's name, photo, two fingerprints, and the card expiration date.

As of May 2018, TSA reported there were 2.2 million active TWICs. The Coast Guard considers TWIC an integral component of the Nation's layered approach to increase port security and protect critical maritime facilities. Paramount to port security is the requirement for MTSA-regulated facilities to develop and implement a comprehensive security plan. The security plan identifies security vulnerabilities and access control measures, such as the use of TWIC, to ensure the physical security and safety of the facility. Other layers of security might include onsite security personnel, cameras, gates, and access badge systems.

MTSA requires the Coast Guard to review and approve each facility security plan. The *Security and Accountability For Every Port Act of 2006* (*SAFE Port Act*) (Public Law 109–347) further mandates that the Coast Guard conduct annual inspections to verify the effectiveness of each facility security plan and ensure the facility is operating in compliance with the approved plan. The Coast Guard reported that as of December 31, 2017, there were 2,470 MTSA-regulated facilities required to have an approved facility security plan.

Results of Audit

DHS did not complete an assessment to evaluate the security value of the TWIC program as required by Public Law 114–278, Section 1(b). This occurred because DHS experienced challenges identifying an office responsible for the effort. As a result, the Coast Guard does not have a full understanding of the extent to which the TWIC program addresses security risks in the maritime environment. This will continue to impact the Coast Guard's ability to properly develop and enforce regulations governing the TWIC program. For example, the Coast Guard did not clearly define the applicability of facilities that have certain dangerous cargo (CDC) in bulk when developing a final rule to implement the use of TWIC readers at high-risk maritime facilities. Without oversight and policy improvements in the TWIC program, high-risk facilities may continue to operate without enhanced security measures, putting these facilities at an increased security risk.

The Coast Guard needs to improve its oversight of the TWIC program to reduce the risk of transportation security incidents. Due to technical problems and lack of awareness of procedures, the Coast Guard did not make full use of the TWIC card's biometric features as intended by Congress to ensure only eligible individuals have unescorted access to secure areas of regulated facilities. During inspections at regulated facilities from fiscal years 2016 through 2017, the Coast Guard only used electronic readers to verify, on average, about 1 of every 15 TWIC cards against TSA's canceled card list. This occurred because the majority of the TWIC readers in the field have reached the end of their service life. Furthermore, the Coast Guard's guidance governing oversight of the TWIC program is fragmented, which sometimes led to confusion and inconsistent inspection procedures. This resulted in fewer regulatory confiscations of TWIC cards.

DHS Needs to Complete Mandated TWIC Program Assessment

DHS did not complete a mandated assessment of the security value of the TWIC program. This occurred because DHS experienced challenges identifying a responsible office. As a result, DHS has not evaluated the extent to which the TWIC program currently addresses security risks in the maritime environment.

In May 2011, the U.S. Government Accountability Office (GAO) recommended[4] that DHS conduct an effectiveness assessment for the TWIC program. According to GAO, conducting this assessment to identify and assess the TWIC program security risks and benefits could better position DHS and policymakers to determine the impact of TWIC on enhancing maritime security. In January 2014, Congress required DHS to complete the assessment in the *Consolidated Appropriations Act, 2014* (Public Law 113–76).

Although DHS completed an effectiveness assessment in January 2016, GAO concluded that it did not substantively address the concerns raised in its report. Consequently, in December 2016, Congress again directed DHS in the *Transportation Security Card Program Assessment Act* (Public Law 114–278, Section 1(b)) to complete the assessment by February 2018. Among other things, the assessment must review the security value of the TWIC program by:

- evaluating the extent to which the program, as implemented, addresses known or likely security risks in the maritime and port environments;
- evaluating the potential for a non-biometric credential alternative;
- identifying the technology, business process, and operational impacts of using TWIC cards and readers in the maritime and port environments;
- assessing the costs and benefits of the program, as implemented; and
- evaluating the extent to which DHS has addressed program deficiencies previously identified by GAO and DHS Office of Inspector General (OIG).

According to DHS, it experienced challenges identifying an office responsible for the effort. Therefore, DHS did not award a contract to start the assessment until February 26, 2018 — more than 6 months after we initiated our audit. Ultimately, the DHS Science and Technology Directorate, in consultation with the Coast Guard and TSA, awarded a contract for the Homeland Security Operational Analysis Center to complete the assessment. The estimated

[4] GAO-11-657, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, May 10, 2011

contract delivery date for the final assessment report is April 2019. If the assessment identifies a deficiency in the effectiveness of the TWIC program, DHS must submit a corrective action plan to Congress no later than 60 days after the assessment has been completed. Public Law 114–278, Section 1(d)(1) also requires DHS OIG to review the plan within 120 days after the date of submission.

Without the DHS assessment and TSA's input, the Coast Guard does not have a full understanding of the extent to which the TWIC program addresses security risks in the maritime environment. This will continue to impact the Coast Guard's ability to properly develop and enforce regulations governing the TWIC program. For example, the Coast Guard has experienced challenges developing a final rule to fully implement the use of TWIC readers at high-risk, MTSA-regulated facilities.

Coast Guard Needs to Clarify TWIC Reader Requirements for Industry

The Coast Guard did not properly develop regulations as mandated by the *SAFE Port Act* to require the use of electronic TWIC readers at all high-risk, MTSA-regulated facilities. Although the Coast Guard issued a TWIC reader final rule, effective August 23, 2018, the final rule did not clearly define facilities that have CDC in bulk subject to the TWIC reader requirements. Consequently, DHS approved the Coast Guard to propose a 3-year partial delay to the final rule, thereby allowing some high-risk facilities to continue operating without enhanced security measures.

After publication of the final rule, the Coast Guard identified potential issues with the final rule's applicability for facilities that have CDC in bulk. Specifically:

- The Coast Guard intended the final rule to apply to the presence of CDC at a facility, regardless of whether the facility transferred CDC to or from a vessel. However, industry initially believed the final rule would only apply to facilities that transferred[5] CDC to or from vessels.

- The Coast Guard concluded its risk analysis methodology did not establish a minimum threshold of CDC quantities or consider other contributing factors that would pose a significant risk at a facility. Other factors would include the geographic location of the CDC within the facility's MTSA footprint and population densities surrounding the facility. Industry estimated that the actual scope of the final rule in this area was about four times larger than the approximately 230 facilities estimated by the Coast Guard.

[5] In MTSA Policy Advisory Council Decision 20-04, *Certain Dangerous Cargo Facilities*, May 6, 2004, the Coast Guard defined CDC facilities as facilities that transfer CDC between a facility and vessel.

In response to these concerns, the Coast Guard recognized the potential need to better clarify the applicability of the final rule for facilities that have CDC in bulk. After consulting with TSA and DHS, the Coast Guard submitted a recommendation to DHS proposing a 3-year partial delay of the final rule. The delay will provide the Coast Guard additional time to reassess the scope of applicable facilities with CDC in bulk that must implement electronic TWIC readers as an access control measure. According to Coast Guard officials, conducting a more detailed risk analysis during the delay will allow them to either validate or determine the need to change the current applicability language in the final rule.

In January 2018, DHS approved moving forward with a 3-year delay to the final rule for facilities that handle CDC in bulk, but do not transfer CDC to or from a vessel. The delay also applied to facilities that receive vessels carrying CDC in bulk, but do not transfer CDC to or from a vessel. The final rule would have gone into effect on August 23, 2018, for those facilities that handle and transfer CDC in bulk to or from a vessel, and for facilities receiving vessels certified to carry more than 1,000 passengers. To delay the final rule, the Coast Guard issued a notice of proposed rulemaking on June 15, 2018.

However, on August 2, 2018, the President signed into law the *Transportation Worker Identification Credential Accountability Act of 2018* (Public Law 115–230). The law prohibits DHS from implementing or revising the TWIC reader final rule, except to extend its effective date, until 60 days after DHS submits to Congress the assessment of the TWIC program as required by Public Law 114–278.

Until the Coast Guard completes a more detailed risk analysis, has the opportunity to review DHS' assessment of the TWIC program, and considers TSA's input, the Coast Guard cannot fully assess which high-risk facilities are operating without enhanced security measures. TSA believes that further delays to implementing TWIC reader requirements present a significant national and transportation security risk.

Coast Guard Needs to Improve TWIC Card Verification Process

Due to technical problems and lack of awareness of procedures, the Coast Guard did not consistently use electronic readers when conducting TWIC card verifications during its inspections at MTSA-regulated facilities. As a result, the Coast Guard is not making full use of the card's biometric security features as intended by Congress to ensure only eligible individuals have unescorted access to secure areas of facilities.

The *SAFE Port Act* requires the Coast Guard to perform one announced annual compliance exam and at least one unannounced security spot check every 12 months at each MTSA-regulated facility. As part of the inspection process, Coast Guard policy[6] requires its inspectors to conduct random TWIC card verifications for individuals with unescorted access in secure areas.

Verification procedures involve electronic checks, when handheld TWIC readers are available, and visual checks for card authentication, card validation, and identity verification. Inspectors should track their TWIC card verification results in the Coast Guard's system of record, the Marine Information for Safety and Law Enforcement (MISLE) system. Table 1 provides a comparison of the electronic and visual TWIC verification procedures.

Table 1: Comparison of Electronic and Visual TWIC Verification Procedures

	Electronic TWIC Verification	Visual TWIC Verification
Card Authentication	Follow challenge and response protocol using the key stored in the card	Inspect the card's overt security features (e.g., hologram)
Card Validation	Check card's expiration date and verify card to TSA's canceled card list to ensure the cardholder: • does not pose a security threat (e.g., disqualifying offenses or change in immigration status) • has not reported the card as lost, stolen, or damaged	Review the card's expiration date
Identity Verification	Perform a biometric one-to-one match of the cardholder's fingerprint to the templates stored in the card	Compare the card's photograph to the cardholder's appearance

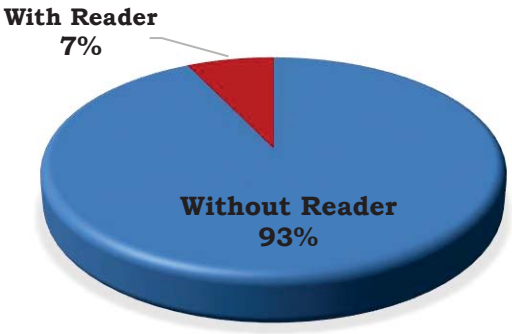
Source: DHS OIG analysis of Coast Guard regulations

In February 2011, the Coast Guard issued guidance reemphasizing the use of TWIC readers as the primary means to verify cards. Electronic verification provides an additional level of security over visual verification by allowing the inspectors to validate the TWIC card against TSA's canceled card list. This ensures that the card is not reported as lost or stolen, and provides assurance that the cardholder has not committed a disqualifying offense, which would result in cancellation or suspension of the card.

[6] Commandant Instruction Manual 16601.1, *Coast Guard TWIC Verification and Enforcement Guide*, October 10, 2008

During FYs 2016 and 2017, the Coast Guard completed 33,800 TWIC verifications at MTSA-regulated facilities, but used electronic readers to verify just 2,425 cards. This represents about 1 in every 15 cards (about 7 percent), as illustrated in figure 1.

Figure 1: TWIC Verifications at MTSA Facilities



Source: OIG analysis of Coast Guard data reported in MISLE as of October 17, 2017 for TWIC verifications at MTSA-regulated facilities

Coast Guard personnel attributed the low TWIC reader usage to the majority of the 250 TWIC readers in the field reaching the end of their service life. In June 2017, the Coast Guard recalled the readers from the field that were no longer used or out of commission. As of August 2017, the Coast Guard estimated there were about 50 to 75 readers operational. The Coast Guard plans to procure 250 replacement readers, valued at $1.7 million, by December 31, 2018.

Other factors that may have contributed to the low TWIC reader usage include:

- Inspectors experienced challenges downloading the canceled card list from TSA's website. Personnel could not connect the readers to the Coast Guard's computer network due to cybersecurity policy restrictions, so they downloaded the list using wireless network connections at public locations.

- Inspectors were not aware of the procedures for entering the results of TWIC reader verifications into MISLE. Although the *Coast Guard TWIC Verification and Enforcement Guide* includes a reference for personnel to document the results according to MISLE User Guides available online, the reference is generic in nature and the online link no longer works.

Without using electronic readers, the Coast Guard did not verify the TWICs against TSA's canceled card list. As of May 2018, there were more than 143,000 TWICs on TSA's canceled card list. Relying on visual verification procedures without the use of electronic TWIC readers reduces the likelihood of identifying individuals who no longer have unescorted access privileges to MTSA-regulated facilities and could pose a security risk.

Coast Guard Needs to Strengthen Oversight Guidance

Coast Guard inspectors did not perform security inspections uniformly across MTSA-regulated facilities. Specifically, the Coast Guard did not document the

confiscation of noncompliant TWIC cards, and inconsistently completed and retained key documents during annual inspections.

Standards for Internal Control in the Federal Government identifies policies and procedures as part of the controls used to ensure agencies meet strategic plans, goals, and objectives. Management should implement control activities by documenting responsibilities in policies and periodically review them for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks.

The *Coast Guard TWIC Verification and Enforcement Guide* governing oversight of the TWIC program is under revision. Interim updates to TWIC program guidance is fragmented across instruction manuals, navigation and vessel inspection circulars, policy letters, policy advisory council documents, informational bulletins, MISLE user guides, and blog posts. Staff rotations and decentralized implementation of additional local procedures at the different Coast Guard Sectors further exacerbate the lack of uniformity of security inspections. Operating in this type of environment leads to confusion and inconsistent practices when confiscating noncompliant TWIC cards and documenting inspection results. As a result, the Coast Guard is reducing the effectiveness of its oversight enforcement for the TWIC program and potentially increasing the security risk in the maritime environment.

Confiscating Noncompliant TWIC Cards

Coast Guard facility inspectors were not fully aware of their authority for confiscating TWIC cards. From FYs 2014 through 2017, the Coast Guard reported in MISLE that it identified more than 1,000 noncompliant TWIC cards during inspections at MTSA-regulated facilities. However, the Coast Guard could not provide documentation showing how many of these cards were confiscated and returned to TSA. Further, during FYs 2014 through 2017, TSA's TWIC Program Office estimated that it received less than a dozen returned cards that it could attribute to the Coast Guard.

This occurred because the Coast Guard's guidance governing oversight of the TWIC program is fragmented. For example:

- In October 2008, guidance issued in the *Coast Guard TWIC Verification and Enforcement Guide* focused on criminal seizure for TWICs. The policy stated facility inspectors may seize a TWIC, if voluntarily surrendered, when probable cause of a crime exists, or the card is altered, fraudulent, counterfeit, stolen, a TWIC of another person, or identified on TSA's canceled card list. However, inspectors shall not attempt to force seizure of a TWIC card.

- In August 2012, guidance issued on *TWIC Enforcement & Procedures for Confiscation* introduced the topic of regulatory confiscation in addition to criminal seizure. The policy stated inspectors shall perform regulatory confiscation if the card appears on TSA's canceled card list, is expired, or is damaged,[7] or when the security features or identity information on the card cannot be recognized. The guidance also included procedures for documenting confiscations in MISLE and returning the cards to TSA.

According to the Coast Guard's Office of Maritime and International Law, Coast Guard facility inspectors are law enforcement personnel and have broad authority[8] to confiscate TWIC cards. Although the August 2012 guidance states that Coast Guard facility inspectors are authorized to perform regulatory confiscation and criminal seizure for TWIC cards, personnel at two of the three sites we visited were not aware of this policy. As a result, personnel at these two sites generally believed that they could only confiscate a TWIC when there was probable cause that the TWIC was evidence of a crime.

Absent clear guidance on regulatory confiscations for TWICs that are listed on TSA's canceled card list, expired, or damaged, these individuals could continually attempt to gain unauthorized access to secure areas of the Nation's critical maritime facilities.

Documenting Security Inspections

Coast Guard inspectors did not consistently document security inspections at MTSA-regulated facilities. Although the Coast Guard generally met the requirements, described here, at the three sites we visited, our review of 67 judgmentally-selected inspections from FYs 2016 and 2017 found inconsistencies with the available documentation:

- Coast Guard inspectors did not retain the completed checklists for 41 of the 67 inspections (about 61 percent). Further, 7 of the 26 inspections with checklists (about 27 percent) were not fully complete. Three of these checklists were for an annual compliance exam that did not have TWIC-related requirements verified as complete.

[7] The Coast Guard issued another policy letter in December 2012 allowing industry to grant unescorted access for up to 37 days to individuals without a TWIC who can provide proof that they have applied and paid for a TWIC renewal (prior to its expiration) or reported their TWIC as lost, stolen, or damaged and are awaiting delivery of a replacement card.
[8] The Coast Guard's law enforcement authority for facilities is in Title 14, United States Code § 99 (see also Commandant Instruction Manual 16247.1G, *Coast Guard Maritime Law Enforcement Manual*, July 19, 2017). In October 2010, Public Law 111–281 authorized the Coast Guard to seize property while conducting port security operations at facilities defined under Title 46, United States Code § 70101.

- Coast Guard inspectors maintained completed documents offline in hardcopy files rather than uploading the documents to the inspection record in MISLE. Although not systemic in nature, maintaining files offline could hinder higher-level oversight and quality assurance reviews.

This occurred because Coast Guard policy does not require its inspectors to complete a standard checklist to ensure that key components of MTSA regulations are verified during annual compliance exams and security spot checks. The checklists are intended as a guide for general MTSA requirements. In addition, although inspectors are required to document inspection results according to MISLE User Guides, the guidance does not include a complete list of minimum supporting documents that must be maintained in the system. For the TWIC program, one part of the overall security inspection process at MTSA-regulated facilities, Coast Guard policy requires inspectors to:

- verify that facility security personnel have the requisite knowledge of TWIC requirements;

- ensure TWIC access control measures are implemented as outlined in the facility security plan for procedures such as granting unescorted access and escorting individuals without a TWIC card; and

- conduct TWIC verifications for individuals with unescorted access to secure or restricted areas.

Inspectors must discuss deficiencies with the facility security officer; take appropriate enforcement action; document the deficiencies on a Form CG-835F, *Facility Inspection Requirements*; record the inspection results in MISLE; and perform follow-up to ensure timely correction of deficiencies.

The Coast Guard's Navigation and Vessel Inspection Circular 03-03, Change 2, *Implementation Guidance for the Regulations Mandated by MTSA for Facilities*, dated February 28, 2009, provides checklists to assist inspectors in conducting annual compliance exams and security spot checks. Inspections also require a review of the facility security plan, interaction with the facility owner and designated security officers, oral examination, observation, and record review.

Without clear guidance for conducting and documenting security inspections, the Coast Guard has limited assurance that inspectors are consistently verifying key requirements of MTSA regulations. If no deficiencies are found during a Coast Guard security inspection, MISLE will only show the general areas with satisfactory results, such as documentation, communication, and operations; and the number of compliant TWIC cards. Detailed information on each specific MTSA requirement verified during the inspection would only be available in an attached checklist. Maintaining the completed inspection

checklist is especially critical to prevent a duplication of effort on consecutive security spot checks. Appropriate coverage for other MTSA requirements provides additional assurance that the facility is operating in compliance with its approved security plan to reduce the risk of a transportation security incident.

Recommendations

Recommendation 1: We recommend the DHS Under Secretary for Science and Technology complete the TWIC program assessment required by Public Law 114–278 to evaluate the security value of the TWIC program.

Recommendation 2: We recommend the Coast Guard's Assistant Commandant for Prevention Policy take action to more clearly define the applicable facilities that have certain dangerous cargo in bulk and which must implement the use of electronic TWIC readers as an access control measure.

Recommendation 3: We recommend the Coast Guard's Assistant Commandant for Prevention Policy improve the Coast Guard's use of electronic TWIC card readers during annual inspections at regulated facilities by procuring new TWIC card readers.

Recommendation 4: We recommend the Coast Guard's Assistant Commandant for Prevention Policy revise and strengthen the *Coast Guard TWIC Verification and Enforcement Guide*. At a minimum, the policy should:

- streamline guidance for oversight of the TWIC program by consolidating requirements from other interim Coast Guard policy documents;

- include more specific procedures for recording the results of electronic TWIC verifications in the Marine Information for Safety and Law Enforcement system, such as updating the reference to the appropriate user guide and requiring inspectors to add a narrative explanation when card readers are not used for verifications;

- define Coast Guard facility inspectors as law enforcement personnel, clarify the inspectors' authority for performing regulatory confiscations of TWIC cards, and outline the required procedures for documenting regulatory confiscations in the Marine Information for Safety and Law Enforcement system and returning the cards to TSA; and

- specify key documents that Coast Guard facility inspectors must upload in the Marine Information for Safety and Law Enforcement system for annual compliance exams and security spot checks at regulated facilities, including but not limited to the completed inspection checklist, Form CG-835F, enforcement actions, and evidence of corrective action taken.

Management Comments and OIG Analysis

The Department concurred with all four recommendations. Appendix A contains a copy of DHS' management comments in their entirety. We also received technical comments and incorporated them in the report where appropriate. A summary of the Department's responses and our analysis follow.

DHS Response to Recommendation 1: Concur. The Homeland Security Operational Analysis Center, administered by the DHS Science and Technology Directorate, is conducting the assessment. When completed, the Science and Technology Directorate will deliver the final report to the Secretary of Homeland Security for follow-up action, as appropriate. The estimated completion date is April 30, 2019.

OIG Analysis: The Department's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the Department provides evidence to support that corrective actions are completed.

Coast Guard Response to Recommendation 2: Concur. The Coast Guard will take action to more clearly define the applicable facilities that have CDC in bulk and which must implement the use of electronic TWIC card readers as an access control measure. The Coast Guard noted that the *Transportation Worker Identification Credential Accountability Act of 2018* prohibits implementing the TWIC reader rule requiring electronic inspections of TWIC until 60 days after DHS has submitted an assessment of the TWIC program to Congress. The DHS assessment, as well as TSA and congressional feedback concerning the results, could affect the Coast Guard's definition of applicable CDC facilities. The estimated completion date is March 30, 2020.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the Coast Guard provides evidence to support that corrective actions are completed.

Coast Guard Response to Recommendation 3: Concur. The Coast Guard is currently working through the procurement process to acquire new TWIC readers for field inspectors. The contract is expected to be awarded by December 31, 2018, subject to the Federal acquisition process. The estimated completion date is March 31, 2019.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the Coast Guard provides evidence to support that corrective action is completed.

Coast Guard Response to Recommendation 4: Concur. The Coast Guard is reviewing all applicable TWIC instructions, policies, and procedures. Revising and strengthening the *Coast Guard TWIC Verification and Enforcement Guide* will require formal rulemaking activities. Consistent with previous rulemaking efforts, the Coast Guard identified a timeline of 3 years for implementing the recommendation. However, it noted that the estimated completion date may also change based on the requirements set forth in the *Transportation Worker Identification Credential Accountability Act of 2018*, other stakeholders' input received after completion of the statutorily required TWIC assessment, and outcomes of pending litigation.

OIG Analysis: The Coast Guard's corrective action is responsive to the recommendation. The recommendation will remain open and resolved until the Coast Guard provides evidence to support that corrective actions are completed. We established an estimated completion date of September 30, 2021.

Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent to which DHS completed an assessment of the security value of the TWIC program as required by Public Law 114−278, Section 1(b). In addition, we determined the extent to which the Coast Guard's oversight of the TWIC program ensures only eligible individuals are granted unescorted access to secure areas of regulated facilities.[9] To answer our objectives, we:

- interviewed officials from the DHS Science and Technology Directorate; Coast Guard's Office of Port and Facility Compliance, Office of Maritime and International Law, Investigative Service, and Domestic Port Security Assessment; and TSA's Office of Intelligence and Analysis and Office of Security Operations to gain an understanding of the TWIC program;

- conducted site visits to the Coast Guard Sectors in Boston, MA; Staten Island, NY; and Houston, TX; observed security inspections at six regulated facilities (four announced annual compliance exams and two unannounced security spot checks); and interviewed the local facility inspectors to gain an understanding of the inspection process controls;

[9] The Coast Guard's oversight of the TWIC program (i.e., developing and enforcing regulations) applies to MTSA-regulated facilities and vessels. However, we limited the audit scope for this engagement to facilities because the Coast Guard identified facilities as a higher risk than vessels.

- analyzed prior audits conducted by DHS OIG and GAO to gain an understanding of the findings, recommendations, and any associated corrective actions involving the TWIC program;

- researched laws, regulations, and internal policies to identify applicable criteria governing the Coast Guard's oversight of the TWIC program;

- analyzed data from the Coast Guard's MISLE system for inspections conducted at MTSA-regulated facilities from FYs 2014 through 2017; and

- assessed the reliability of the MISLE data by performing electronic testing of required data elements, tracing a judgmental sample of records to source documentation, comparing the total number of facilities recorded as inspected to local facility listings, and interviewing Coast Guard officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted this performance audit between August 2017 and May 2018 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

The Office of Audits major contributors to this report are Ruth Blevins, Director; Nick Genitempo, Audit Manager; Marissa Weinshel, Auditor-in-Charge; Robert Orsimarsi, Auditor; Oluwabusayo Sobowale, Auditor; Cassandra Cantu, Program Analyst; Thomas Hamlin, Communications Analyst; and Kevin Donahue, Independent Referencer.

Appendix A
Management Comments to the Draft Report

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

Homeland Security

September 7, 2018

MEMORANDUM FOR: Sondra F. McCauley
Acting Assistant Inspector General for Audits
Office of the Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management Response to OIG Draft Report: "Review of Coast Guard's Oversight of TWIC Program"
(Project No. 17-096-AUD-USCG, TSA)

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

The Transportation Worker Identification Credential (TWIC) is one part of the layered approach to port security and establishes a minimum, uniform, vetting and threat assessment for mariners and port workers across the country. The Coast Guard and the Transportation Security Administration (TSA) have formed a successful partnership in the joint management of the TWIC program and continue to work together to effectively build, manage, and improve it. Specifically:

- TSA is responsible for TWIC enrollment, security threat assessment and adjudication, card production, technology, TWIC issuance, conduct of the TWIC appeal and waiver process as it pertains to credential issuance, and management of government support systems.

- The Coast Guard is responsible for establishing and enforcing access control requirements at Maritime Transportation Security Act (MTSA) regulated vessels and facilities, which include the requirement for TWIC.

DHS remains committed to enhancing the safety and security of the nation's ports through the effective implementation of the TWIC program.

The draft report contained four recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in Project No. 17-096-AUD-USCG, TSA

Recommendation 1: We recommend the DHS Under Secretary for Science and Technology complete the TWIC program assessment required by Public Law 114-278 to evaluate the security value of the TWIC program.

Response: Concur. The Homeland Security Operational Analysis Center operated by the RAND Corporation and administered by the S&T Directorate as a Federally Funded Research Center, is already conducting the assessment. When completed, the final report "Assessing the Risk-Mitigation Value of TWIC at Maritime Facilities," will be delivered to the Secretary of Homeland Security for follow-up action(s), as appropriate. Estimated Completion Date (ECD): April 30, 2019.

Recommendation 2: We recommend the Assistant Commandant for Prevention Policy take action to more clearly define the applicable facilities that have CDC [certain dangerous cargo] in bulk and which must implement the use of electronic TWIC readers as an access control measure.

Response: Concur. The Coast Guard Office of Port and Facility Compliance will take action to more clearly define the applicable facilities that have CDC in bulk and which must implement the use of electronic TWIC readers as an access control measure. It is important, however, to note that on August 2, 2018, the President of the United States signed into law the "TWIC Accountability Act of 2018." This law prohibits the Coast Guard from implementing the TWIC reader rule requiring electronic inspections of TWIC until 60 days after DHS has submitted an assessment of the TWIC program to Congress. DHS' assessment which is currently being conducted by HSOAC (expected to be complete by April 30, 2019), and TSA and possible Congressional feedback concerning that assessment (expected by June 30, 2019), could affect the Coast Guard's definition of applicable CDC facilities. ECD: March 30, 2020.

Recommendation 3: We recommend the Assistant Commandant for Prevention Policy improve the Coast Guard's use of electronic TWIC card readers during annual inspections at MTSA-regulated facilities by procuring new TWIC card readers.

Response: Concur. Coast Guard Office of Port and Facility Compliance personnel are currently working through the procurement process to acquire new TWIC readers for field inspectors. The contract is expected to be awarded by December 31, 2018, subject to the federal acquisition process. ECD: March 31, 2019.

Recommendation 4: We recommend the Assistant Commandant for Prevention Policy revise and strengthen the "Coast Guard TWIC Verification and Enforcement Guide." At a

3

minimum, the policy should:

- streamline guidance for oversight of the TWIC program by consolidating requirements from other interim Coast Guard policy documents;
- include more specific procedures for recording the results of electronic TWIC verifications in the Marine Information for Safety and Law Enforcement (MISLE), such as updating the reference to the appropriate MISLE User Guide and requiring inspectors to add a narrative explanation when card readers are not used for verifications;
- define Coast Guard facility inspectors as law enforcement personnel, clarify the inspectors' authority for performing regulatory confiscations of TWIC cards, and outline the required procedures for documenting regulatory confiscations in MISLE and returning the cards to TSA; and
- specify key documents that Coast Guard facility inspectors must upload in MISLE for annual compliance exams and security spot checks at MTSA-regulated facilities, including but not limited to the completed inspection checklist, CG-835, enforcement actions, and evidence of corrective action taken.

Response: Concur. Coast Guard Office of Port and Facility Compliance personnel are currently in the process of reviewing all applicable TWIC instructions, policies, and procedures. Revising and strengthening the "Coast Guard TWIC Verification and Enforcement Guide" will require formal rulemaking activities. The ECD for this will be consistent with the Coast Guard's "Notice of Proposed Rule Making," (2017-USCG-0711), dated June 22, 2018, (see: https://www.gpo.gov/fdsys/pkg/FR-2018-06-22/pdf/2018-13345.pdf) which identifies a timeline of three years. This ECD may also change based on the requirements set forth in the "TWIC Accountability Act of 2018," other stakeholders input received after completion of the statutorily required TWIC assessment, and outcomes of pending litigation. ECD: To Be Determined.

4

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
TSA Administrator
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commandant, United States Coast Guard
United States Coast Guard Audit Liaison
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305