



July 2026

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL

Actions Needed to Address Maritime Security Risks



A report to congressional addressees.

For more information, contact: Tina Sherman at shermant@gao.gov.

What GAO Found

TSA has taken some steps to communicate Transportation Worker Identification Credential (TWIC®) program information with stakeholders. However, TSA relies on an ad hoc communication approach rather than a documented communication plan to determine how to share information with stakeholders. This has contributed to some stakeholders reporting that they experienced declining engagement with and delays receiving key program updates from TSA. Developing and implementing a communication plan could help TSA ensure that all stakeholders receive the information necessary to effectively operate the TWIC® program and reduce security risks.

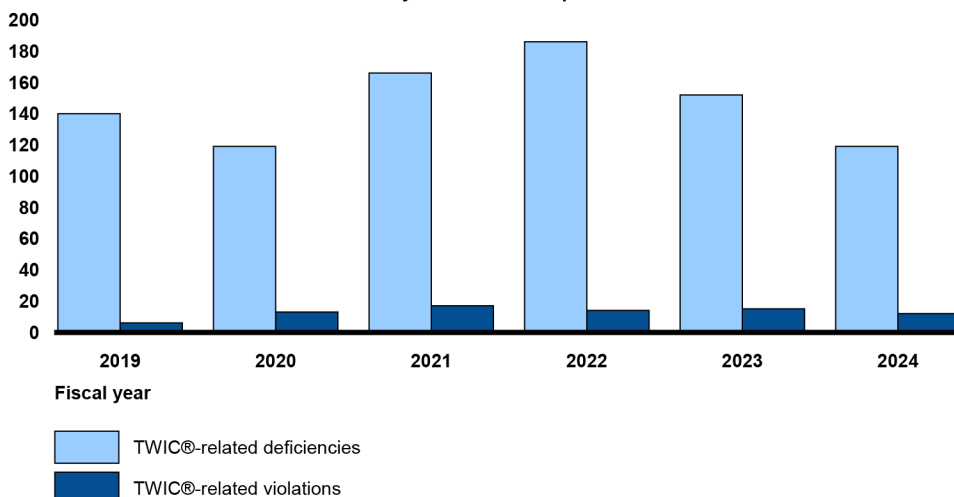
The Coast Guard does not share or analyze all of the data it collects during inspections to oversee how facility operators implement the TWIC® program. For example, the Coast Guard collects data on deficiencies, a less severe form of noncompliance, and violations, a more severe form of noncompliance that can result in notices of violation or civil penalties. GAO's assessment of inspection findings for fiscal years 2019 through 2024 showed:

- 888 TWIC®-related deficiencies, such as operators not ensuring that facility personnel with security duties were qualified to perform their roles, and
- 83 TWIC® violations, such as unescorted individuals entering a secure area, highlighting areas that may warrant improvement.

However, the Coast Guard does not provide the data to TWIC® inspectors. According to officials, this is because the data did not relate to areas that would require a change to the program. However, by communicating the data with inspectors, regardless of their effect on the program, the Coast Guard could improve inspectors' awareness of TWIC®-related risks.

Total Number of Transportation Worker Identification Credential (TWIC®)-related Deficiencies and Violations, Fiscal Years 2019–2024

Number of deficiencies or violations found by Coast Guard inspectors



Source: GAO analysis of TWIC® deficiency and violation data. | GAO-26-107521

Why GAO Did This Study

The TWIC® program aims to provide a tamper-resistant biometric card to maritime workers who require unescorted access to designated secure areas of facilities and vessels under Maritime Transportation Security Act of 2002 regulations. As of August 2025, more than 2 million individuals held a TWIC® credential.

TSA oversees TWIC® applicants' enrollment and background checks. The Coast Guard enforces certain TWIC® regulatory requirements, including by inspecting facilities for compliance.

The Transportation Security Screening Modernization Act of 2024 includes a provision for us to review TSA's security threat assessment programs and we were asked to review other aspects of TWIC® operations. This report examines (1) the extent to which TSA communicates TWIC® program information to stakeholders, and (2) the extent to which the Coast Guard has overseen the implementation of the TWIC® program by facility operators, among other objectives.

GAO also examined TSA and Coast Guard policy and data for fiscal years 2019 through 2024. In addition, GAO interviewed agency officials and port stakeholders. To obtain a range of TWIC® perspectives, these stakeholders included TWIC® operators at facilities selected in part for diversity in size and geographic regions.

What GAO Recommends

GAO is making seven recommendations, including that the TSA Administrator implement a plan to communicate TWIC® information to stakeholders and that the Coast Guard communicate TWIC®-related violation and deficiency data with inspectors. The Department of Homeland Security concurred with these recommendations.

Contents

Letter		1
	Background	5
	TSA Has Taken Some Steps to Communicate Program Information to Stakeholders, But Has Not Done So Systematically	13
	Coast Guard Oversees Facility Operators' Implementation of TWIC® through Inspections but Gaps Exist in Its Processes	16
	Coast Guard and TSA Have Not Coordinated Their Acquisition of Inspection Devices to Validate TWIC® Cards	29
	Coast Guard Does Not Have a Plan for Finalizing Which Facilities Must Have TWIC® Biometric Card Readers	34
	Conclusions	38
	Recommendations for Executive Action	39
	Agency Comments and Our Evaluation	40
Appendix I	Objectives, Scope, and Methodology	41
Appendix II	Transportation Security Administration's (TSA) Efforts to Streamline TWIC®	45
Appendix III	States and Territories with Comparability for the Hazardous Materials Endorsement (HME)	56
Appendix IV	Performance Measurement System for the Transportation Worker Identification Credential (TWIC®)	59
Appendix V	Timeline for Transportation Worker Identification Credential (TWIC®) Reader Implementation	64
Appendix VI	Comments from the Department of Homeland Security	68

Tables

Table 1: Examples of Transportation Worker Identification Credential (TWIC®)-related Deficiencies Cited in 10 Percent or More of U.S. Coast Guard Inspections of Approximately 3,400 Maritime Transportation Security Act-regulated Facilities from Fiscal Years 2019-2024	18
Table 2: Summary of TWIC® and HME Fee-setting for Fiscal Years 2024 and 2025	55
Table 3: Examples of Performance Measures for the Transportation Worker Identification Credential (TWIC®) Program	59
Table 4: Percentage of TWIC® Enrollments Processed by Rural TSA Enrollment Centers in Selected States	62
Table 5: Transportation Worker Identification Credential (TWIC®) Card Reader Timeline for Regulated Facilities	64

Figures

Figure 1: Transportation Security Agency's (TSA) Process for Individuals to Obtain and Hold a Transportation Worker Identification Credential (TWIC®)	7
Figure 2: Types of Maritime Transportation Security Act-regulated Facilities	10
Figure 3: Functions of a Facility Operator's Transportation Worker Identification Credential (TWIC®) Reader	12
Figure 4: Coast Guard Inspection of Maritime Transportation Security Act-regulated Facility	16
Figure 5: Coast Guard Transportation Worker Identification Credential (TWIC®)-related Inspection Activities	17
Figure 6: Transportation Worker Identification Credential (TWIC®)-related Violations as a Share of All Coast Guard Facility Inspection Violations for the Approximately 3,400 MTSA-regulated Facilities, Fiscal Year 2019-2024	20
Figure 7: Types of Transportation Worker Identification Credential (TWIC®)-related Violations the Coast Guard Recorded for Inspections Conducted, Fiscal Years 2019–2024	21
Figure 8: Total Number of Transportation Worker Identification Credential (TWIC®)-related Deficiencies and Violations	

for the Approximately 3,400 MTSA-regulated Facilities, Fiscal Years 2019-2024	23
Figure 9: Geographic Dispersion of 83 Transportation Worker Identification Credential (TWIC®)-related Violations Coast Guard Recorded for Inspections for the Approximately 3,400 Maritime Transportation Security Act of 2002 (MTSA)-regulated Facilities in Fiscal Years 2019–2024	25
Figure 10: Coast Guard Servicemember Verifies Transportation Worker Identification Credential (TWIC®) Manually; Legacy Coast Guard TWIC® Reader	30
Figure 11: Transportation Security Administration (TSA) Inspector Smart Phone and Associated Plug-In Transportation Worker Identification Credential (TWIC®) Card Reader Device	31
Figure 12: U.S. States and Territories with Comparability for Hazardous Materials Endorsement (HME) for Applicants with an Existing Transportation Worker Identification Credential (TWIC®)	57
Figure 13: Enrollment Center Visit Survey Results for Transportation Worker Identification Credential (TWIC®) Applicants from Fiscal Year 2023 to July 2025	63

Abbreviations

CFATS	Chemical Facilities Anti-Terrorism Standards
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
HME	Hazardous Materials Endorsement
MTSA	Maritime Transportation Security Act of 2002
TSA	Transportation Security Administration
TWIC®	Transportation Worker Identification Credential

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



July 28, 2026

The Honorable Ted Cruz
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Andrew Garbarino
Chairman
The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Carlos A. Gimenez
Chairman
Subcommittee on Transportation and Maritime Security
Committee on Homeland Security
House of Representatives

Ports, waterways, and vessels handle billions of dollars in cargo annually, and an attack on our nation's maritime transportation system could have dire consequences. The 299 domestic maritime ports in the United States are essential elements of the global supply chain. The Maritime Transportation Security Act of 2002 (MTSA) established multiple measures for maritime security, including the Transportation Worker Identification Credential (TWIC®) program.¹ The TWIC® program provides a tamper-resistant biometric card to maritime workers who require unescorted access to designated secure areas of facilities and vessels under MTSA regulations.² As of June 2025, more than 2 million individuals held a TWIC® card.

The Department of Homeland Security (DHS) has two components that oversee the TWIC® program—the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA oversees applicants' enrollment

¹See The Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, tit. I, § 102(a), 116 Stat. 2064, 2073-74 (codified as amended at 46 U.S.C. § 70105).

²See 33 C.F.R. § 101.514; see generally 33 C.F.R. pts. 101, 104, 105, 106.

and the security threat assessment processes.³ The Coast Guard enforces regulations related to TWIC® usage and facility access controls, including the implementation of TWIC® biometric card readers (TWIC® readers) at certain MTSA-regulated facilities.⁴ Both components also have roles on-site at maritime facilities, as each can send inspectors to check that workers' TWIC® cards are valid.

TWIC® stakeholders—port facility operators, industry associations, and a labor union—have expressed several concerns about TWIC® program administration.⁵ These generally relate to TSA's communication with stakeholders and the Coast's Guard's implementation of TWIC® readers.⁶

The Transportation Security Screening Modernization Act of 2024 includes a provision for us to review the administration of the security threat assessment programs by TSA.⁷ We were asked to review other aspects of the TWIC® program. This report examines the following:

1. The extent to which TSA has communicated TWIC® program information to stakeholders.
2. The extent to which the Coast Guard has overseen the implementation of the TWIC® program by facility operators.
3. The extent to which TSA and the Coast Guard have coordinated to acquire devices for purposes of inspecting TWIC® cards for validity.

³TSA is to conduct security threat assessments to determine whether applicants pose a security risk warranting denial of the TWIC credential. See 46 U.S.C. § 70105(b), (c); 49 C.F.R. § 1572.21.

⁴For the purposes of this report, "MTSA-regulated facilities" are those which are subject to 33 C.F.R. part 105, including those which receive vessels certificated to carry more than 150 passengers (except those vessels not carrying and not embarking or disembarking passengers at the facility) and those which receive foreign cargo vessels greater than 100 gross register tons. 33 C.F.R. § 105.105(a).

⁵Port terminal and facility operators are one group of relevant industry stakeholders, or end users, for the TWIC® program. These may be companies or individuals who own or operate a MTSA-regulated port terminal or facility. The term "facility operator" will be used to refer to port terminal and facility owners and operators and the term "stakeholders" will be used to refer to the entire group of relevant stakeholders. See 33 C.F.R. §§ 101.105, 105.100.

⁶We also report on TSA's efforts to streamline TWIC® with other transportation credentialing programs in Appendix II.

⁷Pub. L. No. 118-202, § 4, 138 Stat. 2688, 2690-91.

-
4. The implementation status of TWIC® biometric card readers.
 5. TWIC® fee-setting and efforts to consolidate the TWIC® program with other transportation credentialing programs.

To understand TSA's communication approaches for disseminating TWIC® program information to stakeholders, we reviewed documentation such as TSA's technical advisories. We also interviewed TSA officials regarding any changes to program operations from fiscal years 2019 through 2024 and the steps taken to communicate these changes. To assess how effectively TSA communicated with stakeholders, we interviewed industry representatives from six organizations whose members and affiliates hold TWIC® credentials to obtain their perspectives. We selected these based on the type of membership (e.g., chemical facility operators) and whether they provided feedback on TWIC® to Congress, TSA, and the Coast Guard. We obtained additional perspectives by interviewing members of a nongeneralizable sample of 10 Area Maritime Security Committees selected for their larger size and wider range of port operations, the volume of TWIC® enrollments they represented, and the geographic areas they covered.⁸ We assessed the TSA's communication practices against *Standards for Internal Control in the Federal Government*, which include best practices for communication with external stakeholders.⁹

To understand how the Coast Guard oversees facility operator compliance with TWIC® regulatory requirements and mitigate any TWIC®-related risks, we reviewed Coast Guard documentation of MTSA-regulated facility inspections and TWIC® guidance for facility operators as well as TWIC®-related enforcement data from fiscal years 2019 through 2024.¹⁰ To assess the reliability of these data, we reviewed documentation such as the user guide for the Coast Guard's Marine Information for Safety and Law Enforcement database and interviewed

⁸MTSA provided for the establishment of Area Maritime Security Committees. Pub. L. No. 107-295, § 102(a), 116 Stat. at 2081 (codified as amended at 46 U.S.C. § 70112). These committees provide a link for contingency planning, development, review, and update of Area Maritime Security Plans and to enhance communication between port stakeholders within federal, state, and local agencies and industry to address maritime security issues.

⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-25-107721](#) (Washington, D.C.: May 15, 2025).

¹⁰Coast Guard inspectors can recommend that notices of violation or civil penalties be issued for instances in which a MTSA-regulated facility operator has not complied with TWIC® regulatory requirements, such as for expired TWIC® cards or individuals entering secure facility areas without a TWIC® escort. See 33 C.F.R. § 1.07-11.

Coast Guard officials regarding quality assurance controls for these data. We determined these data to be sufficiently reliable for reporting on TWIC® noncompliance trends.

We also visited a port with MTSA-regulated facilities, selected in part for its large volume of commodities, to interview Coast Guard inspectors and observe a Coast Guard inspection for TWIC® compliance. We compared the Coast Guard's TWIC® enforcement efforts and outcomes against its *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* to assess how it measures TWIC® compliance and addresses risk.¹¹

To assess the extent to which TSA and the Coast Guard have coordinated to acquire devices for purposes of inspecting TWIC® cards for validity, we reviewed acquisition documentation, such as TSA and Coast Guard statements of work for purchased services. We also interviewed TSA and Coast Guard contracting officials about efforts related to their acquisition of TWIC® inspection devices and any potential benefits to coordinating acquisitions and discussed this issue with officials in DHS's Office of the Chief Procurement Officer.

To address the status of TWIC® reader implementation, we analyzed TWIC® biometric card reader requirements in the SAFE Port Act, the Coast Guard's proposed and issued regulations, and related Coast Guard documentation from fiscal years 2006 through 2025, which included the year DHS was first required to conduct a TWIC® reader program.¹² We also interviewed Coast Guard officials and TWIC® stakeholders to identify any concerns with the implementation of TWIC® readers, including the Coast Guard's proposed TWIC® reader rules. We also discussed TWIC® stakeholder views on the costs and challenges associated with Coast Guard rulemaking. While the perspectives we obtained during our interviews are not generalizable, they provide

¹¹United States Coast Guard Deputy Commandant of Operations, *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* (July 2020).

¹²The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) required the Secretary of the department in which the Coast Guard was operating to conduct a TWIC® reader pilot program and promulgate within 2 years of initiating this program the final regulations requiring the deployment of TWIC® readers. Pub. L. No. 109-347, tit. I, § 104, 120 Stat. 1884, 1889-90. For more information, see table 3 and appendix V.

important insights about TWIC® program operations. Appendix I provides more information on our objectives, scope, and methodology.

We conducted this performance audit from April 2024 to July 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Within DHS, TSA and the Coast Guard jointly administer the TWIC® program.

TSA's Role

TSA's Enrollment Services and Vetting Program oversees TWIC® applicants' enrollment as well as TSA's contract with enrollment center staff.¹³ TSA's Office of Intelligence and Analysis determines through the adjudication process if TWIC® applicants' background checks return information that would disqualify them from a TWIC® card, according to TSA officials. As figure 1 illustrates, the adjudication process involves TSA reviewing and approving required information, including fingerprints and documents to establish identity and citizenship. It also involves checks of the applicant's information against various databases, including the Next Generation Identification System.¹⁴

If these checks do not return any disqualifying information, TSA then approves the applicant for a TWIC® card.¹⁵ If TSA finds disqualifying information, it sends the applicant a preliminary determination of ineligibility describing why the applicant is ineligible for a TWIC® card and

¹³TSA contracted with a private entity to operate its enrollment centers.

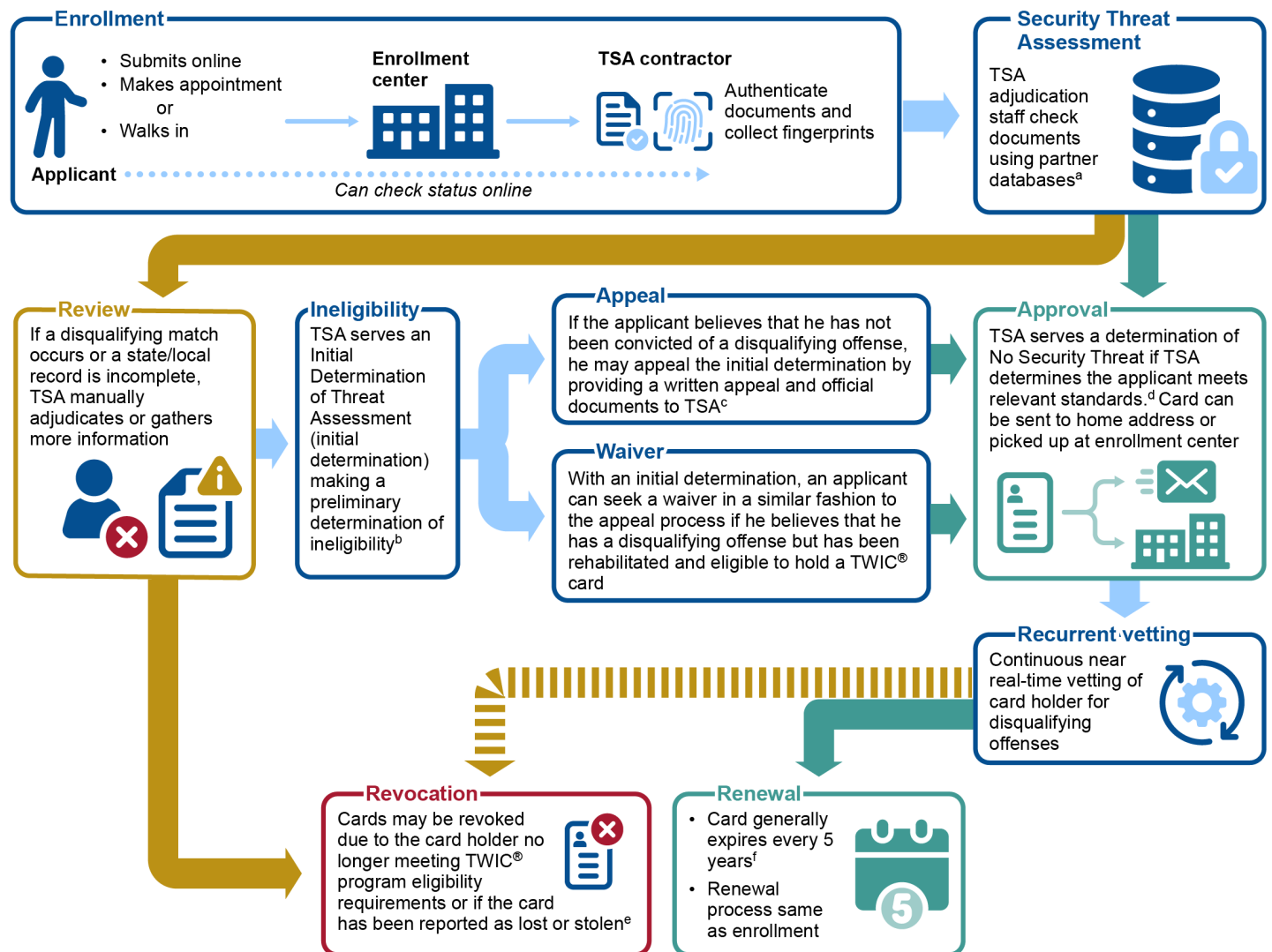
¹⁴The Federal Bureau of Investigation maintains the Next Generation Identification System which is a cooperative federal-state system for the exchange of fingerprint-supported criminal history records, including those records that are voluntarily submitted by state repositories, Tribes, and federal agencies.

¹⁵TSA may permanently disqualify TWIC® applicants if they were convicted, pled guilty (including 'no contest'), or found not guilty by reason of insanity for 12 permanently disqualifying offenses, including murder and crimes involving terrorism or transportation security incidents, regardless of when they occurred. TSA may also temporarily disqualify TWIC® applicants for a variety of reasons, including if they were convicted or found not guilty by reason of insanity for any of 15 interim disqualifying offenses, including arson and assault with intent to kill, if the applicant was convicted of the offense within 7 years or released from incarceration within 5 years of the application date. 46 U.S.C. § 70105(c).

outlining methods of redress (appeal or pursuit of waiver).¹⁶ TSA also collects a non-refundable enrollment fee.

¹⁶As part of TWIC® redress, applicants may request an appeal, a waiver, or both. TSA is to consider the following five criteria when determining whether to grant a waiver for a disqualifying criminal offense, as applicable: circumstances of the disqualifying act or offense; restitution made by the applicant; any federal or state mitigation remedies (such as certificates showing completion of court-ordered substance abuse or other treatment programs); court records or official medical release documents indicating the applicant no longer lacks mental capacity; and, any other factors that indicate the applicant does not pose a security threat warranting denial of the credential. 46 U.S.C. § 70105(c)(2); 49 C.F.R. § 1515.7(c)(2).

Figure 1: Transportation Security Agency's (TSA) Process for Individuals to Obtain and Hold a Transportation Worker Identification Credential (TWIC®)



Source: GAO analysis of TSA documentation; Icons_Studio/stock.adobe.com. | GAO-26-107521

^aPartner databases include terrorist screening, immigration, and criminal history databases.

^b49 C.F.R. § 1572(d)(2). According to TSA, if the card holder cannot successfully complete the Preliminary Determination of Ineligibility or elects not to respond, the card is revoked and placed on the Canceled Card List.

^c49 C.F.R. pt. 1515.

^d49 C.F.R. § 1572(d)(1).

^eSee 49 C.F.R. § 1572.5(b).

^f49 C.F.R. § 1572.23(a).

A TWIC® card is generally valid for 5 years, or the period in which the background check is valid. TWIC® recurrent vetting provides near real-time continuous monitoring of the eligibility status of approved TWIC® applicants for the length of the valid security threat assessment. TSA places TWIC® holders on the Canceled Card List if the agency rules them ineligible due to disqualifying offenses, such as having a criminal conviction for murder or reporting the card as lost or stolen.

Pursuant to regulations issued by DHS under the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA has the authority to assess civil penalties for TWIC®-related violations.¹⁷ TSA Surface Inspectors can check to ensure that individuals in secure areas of MTSA-regulated facilities have valid TWIC® cards. Both Coast Guard inspectors and TSA Surface Inspectors visually examine and use devices to verify the validity of TWIC® cards at MTSA-regulated facilities. Coast Guard inspectors previously used handheld TWIC® readers and TSA inspectors use government-issued smart phone devices with a reader application and plug-in device.

TSA oversees several credentialing programs in addition to TWIC®, which aim to reduce security threats to United States' air and surface transportation systems. These include the Hazardous Materials Endorsement (HME) and TSA PreCheck®.

- Federal law requires HME certification on a commercial driver's license for drivers to legally transport certain hazardous materials in the U.S.¹⁸ While TSA administers the security threat assessment, states issue the HME certification on commercial driver's licenses.
- TSA PreCheck® is a voluntary enrollment program that eligible travelers may enroll in to receive expedited security screening at participating U.S. airports.

According to TSA, as of December 2025, about 2.3 million individuals have a TWIC®, 1.2 million individuals have an HME, and 21 million individuals are active TSA PreCheck® members. TSA has implemented

¹⁷Section 1302(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 gave the Secretary of Homeland Security the authority to assess civil penalties for violations of regulations issued by the Secretary under surface transportation requirements of title 49 of the U.S. Code and chapter 701 of title 46 of the U.S. Code, which, among other things, include provisions related to TWIC®. Pub. L. No. 110-53, tit. XIII, § 1302(a), 121 Stat. 266, 390-92 (codified as amended at 49 U.S.C. § 114(u)).

¹⁸49 C.F.R. § 383.93(b)(4).

some streamlining methods, partially in response to stakeholder concerns, for applicants who may need more than one of these credentials, according to TSA officials. See Appendix II for more information.

MTSA Requirements for Facility Security Plans and Coast Guard's Role to Ensure Compliance

MTSA-regulated facilities and the Coast Guard have intertwined roles in implementing TWIC® regulatory requirements. Many ports have both MTSA- and non-MTSA-regulated facilities that store a range of commodities, such as liquid bulk cargo (oil and chemicals), according to Coast Guard officials. Some facilities—such as those handling liquefied natural and hazardous gas and transferring oil or hazardous material in bulk—are subject to MTSA regulations.¹⁹ According to the Coast Guard, there are about 3,400 facilities subject to these regulations. If a facility is subject to MTSA regulations, it must have a facility security plan that addresses how certain TWIC® regulatory requirements will be met. The Coast Guard reviews and approves the plan every five years or if the facility operator amends the plan, in addition to conducting site visits to the facilities to verify the effectiveness of the plan.²⁰

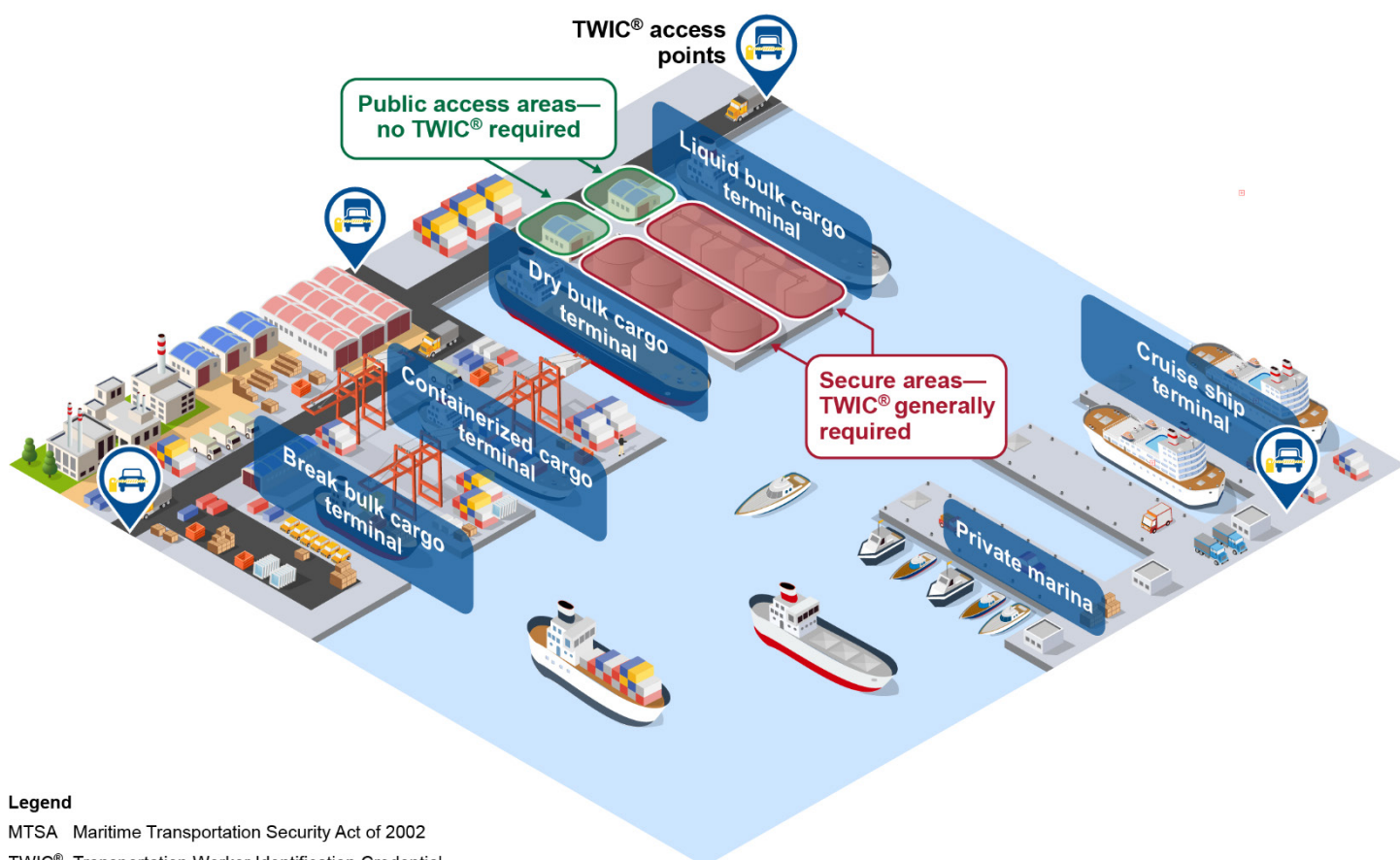
Facility security officers must specify within these plans which areas of their facilities are secure, generally requiring TWIC® cards to access.²¹ For example, the facility security officer could designate the lobby or administrative spaces of a MTSA-regulated facility as not secure and, therefore not subject to TWIC® regulatory requirements (see fig. 2). MTSA regulations also require facility operators to describe in these plans how they will incorporate TWIC® into their access control system for the facility.

¹⁹33 C.F.R. § 105.105(a), pts. 127 and 154.

²⁰46 U.S.C. § 70103(c)(4); 33 C.F.R. §§ 105.410(c), (f).

²¹Additionally, regulations refer to “restricted” areas in some instances as generally requiring TWIC® cards to access. See 33 C.F.R. § 101.105 (using terms “secure” and “restricted” in the TWIC® “escorting” definition interchangeably); but see 33 C.F.R. § 105.200(b)(6)-(7) (requiring TWIC® cards in “restricted areas” only if applied to such areas).

Figure 2: Types of Maritime Transportation Security Act-regulated Facilities



Legend

MTSA Maritime Transportation Security Act of 2002

TWIC® Transportation Worker Identification Credential

Source: GAO analysis of port information; AlexZel/stock.adobe.com (port illustration). | GAO-26-107521

Note: See Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, tit. I, § 102(a), 116 Stat. 2064, 2073-74 (codified as amended at 46 U.S.C. § 70105). For the purposes of this figure, "Maritime Transportation Security Act-Regulated Facilities" are those in 33 C.F.R. § 105.105(a).

Since 2009, the Coast Guard promulgated rules²² concerning facilities' implementation of TWIC® readers for facilities designated as high-risk

²²Promulgate is the formal process of rulemaking by publishing the proposed regulation, inviting public comments, and approving or rejecting the proposal.

facilities within TWIC® regulatory requirements.²³ MTSA regulations define high-risk facilities to include those that receive vessels certificated to carry 1,000 or more passengers, such as cruise ship terminals, as well as those that handle Certain Dangerous Cargoes in bulk, such as certain chemicals.²⁴ Currently, Coast Guard regulations only require facilities that receive vessels certificated to carry 1,000 or more passengers to have TWIC® readers.²⁵ According to the Coast Guard, this category currently only includes cruise ship terminals because the agency is re-evaluating how they determine the risk level and potential applicability of the TWIC® reader requirements to MTSA-regulated facilities that handle Certain Dangerous Cargoes in bulk. Coast Guard regulations will require other high-risk MTSA-regulated facilities, such as those that handle Certain Dangerous Cargoes in bulk, to implement the TWIC® readers in 2029.²⁶ Rulemaking for these other facilities has been delayed, as discussed later in this report.

TWIC® readers can be permanently attached to a facility's entryway, such as on turnstiles, or can be portable, handheld devices that security staff would use, as shown in figure 5. Either way, the readers confirm that the TWIC® card (1) is authentic (i.e., TSA issued); (2) has not expired; and (3) is not on the Canceled Card List. Additionally, the card readers

²³In 2013, we found that the TWIC® biometric card reader pilot results were unreliable and that the program's benefits need to be reassessed. We recommended a matter for congressional consideration that Congress direct DHS to assess the effectiveness of the TWIC® readers and develop a final regulation based on the assessment. GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, [GAO-13-198](#) (Washington D.C.: May 8, 2013). In 2014, Congress directed DHS to complete this assessment, and the Coast Guard commissioned a 2022 Homeland Security Operational Analysis Center study providing a risk-informed analysis of the TWIC® readers. 160 Cong. Rec. H475 (daily ed. Jan. 15, 2014) (accompanying Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5). Since they were first proposed by Coast Guard in 2009, regulations implementing the TWIC® program have categorized MTSA-regulated facilities into risk groups, with the highest risk group labeled "Risk Group A." For the purposes of this report, "high-risk" MTSA-regulated facilities are those defined as "Risk Group A" in 33 C.F.R. § 105.253(a)(1)-(4), which includes facilities that will only be subject to "Risk Group A" regulations in 2029. Currently, only facilities that receive vessels certificated to carry more than 1,000 passengers are subject to these regulations. However, beginning in May 2029, more types of facilities will be subject to the "Risk Group A" regulations. See Appendix V for more information on laws, regulations, and GAO recommendations regarding MTSA-regulated facilities.

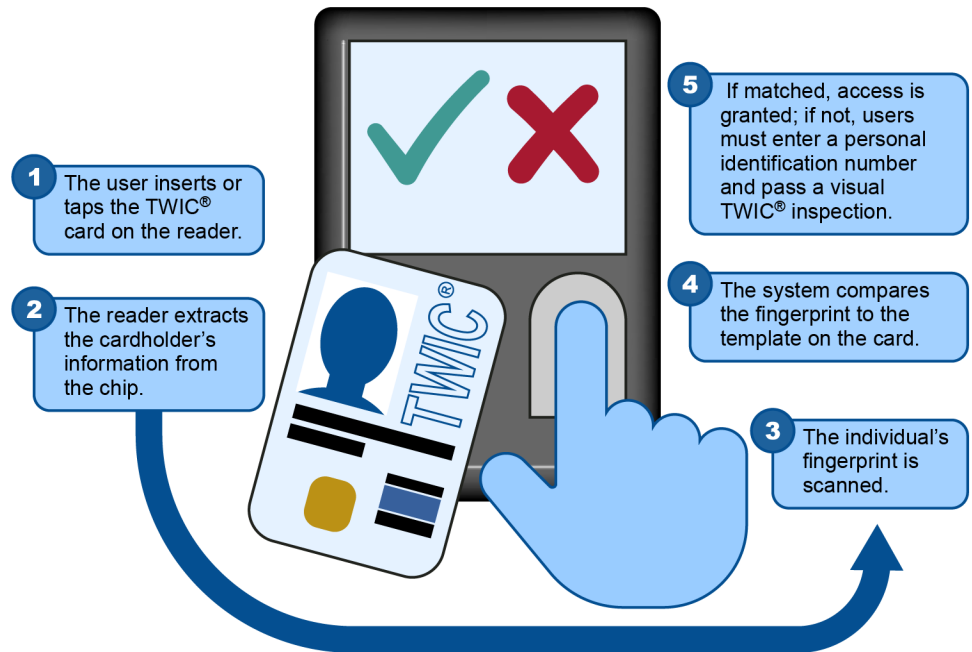
²⁴33 C.F.R. § 105.253(a). See 33 C.F.R. §§ 101.105, 160.202.

²⁵33 C.F.R. §§ 101.520, 101.535(b), 105.253(a)(1).

²⁶33 C.F.R. § 105.253(a).

confirm that the fingerprints of the person presenting the card match the person's fingerprints in TSA's credentialing system. Figure 3 shows how the facility TWIC® readers function, using contact or contactless technology along with the card holder's fingerprint to validate TWIC® cards. If individuals are unable to provide valid fingerprints, they must enter a personal identification number and pass a visual TWIC® inspection.²⁷

Figure 3: Functions of a Facility Operator's Transportation Worker Identification Credential (TWIC®) Reader



Source: GAO analysis of TWIC® reader information; Icons-Studio/stock.adobe.com (hand). | GAO-26-107521

²⁷Card holders with the new version of the TWIC® card—the NEXGEN TWIC®—do not need to use a personal identification number since the reader can verify the card using only the facial image, according to TSA officials.

TSA Has Taken Some Steps to Communicate Program Information to Stakeholders, But Has Not Done So Systematically

TSA has taken some steps to communicate with stakeholders. They disseminated information to TWIC® program stakeholders and collected feedback from them. For example, in 2007, TSA established a TWIC® Stakeholder Communications Committee that consisted of stakeholders in the maritime industry, union representatives, and other related groups. The committee's goal was to have a centralized means of disseminating program updates and information relevant for TWIC® users, such as the appeals process for their security threat assessment. According to TSA officials, the group stopped meeting due to COVID-19 in 2022. TSA officials reconvened this Committee in September 2025 with plans to meet on a six-month basis in the future.

Further, TSA officials told us they are currently redesigning TSA's public website to include resources, such as technical advisories, that industry stakeholders can more easily access. As of December 2025, TSA officials told us that they plan to add these beginning in January 2026 but have experienced some minor technical difficulties in some of their redesign work thus far.

TSA also has several ways to collect stakeholder feedback: optional customer satisfaction surveys for applicants after their visit to an enrollment center, an email account to which anyone can write expressing concerns or asking questions, and a toll-free help desk line that can provide updates about enrollment center availability and individuals' application status.²⁸ TSA officials also told us they routinely engage with stakeholders at conferences; during webinars about TWIC®, which TSA hosts; and industry committee meetings as well as meet with them on an ad hoc basis. TSA collects this feedback as part of its broader performance measurement activities, as outlined in Appendix IV.

However, TSA's communication approaches have been ad hoc and not informed by a communication plan. TSA officials said that they keep a record of all its TWIC® meetings with stakeholders, including ones from industry, that includes the date and the location, and that they discuss stakeholder engagement practices weekly. However, TSA does not have a communication plan to guide, for example, what information is key to share or who should receive the information when. In the absence of a communication plan to guide its efforts, TSA also has not systematically

²⁸According to TSA officials, 90 percent of inquiries they have received are applicants requesting a case status update rather than sharing feedback on program operations.

determined how to communicate the information and which communication vehicles can reach the greatest number of stakeholders.

Industry associations, facility operators, and Coast Guard officials with whom we spoke reported some concerns with TSA's communication, underscoring frustration with ad hoc approaches. These include their experiences with TSA's declining engagement, and delays receiving key program updates.

Declining engagement. Five out of six industry associations said they experienced, over time, either a decline in or a deficient level of communication with TSA on TWIC® despite previously either having strong working relationships with TSA or receiving regular information on TWIC® from TSA. One industry association stakeholder said that during the initial TWIC® rollout in 2007, they received quarterly program updates from TSA's Highway Motor Carrier Sector Coordinating Council meetings, but they said TSA no longer holds these meetings. Further, facility operators representing 5 of the 10 Area Maritime Security Committees we spoke with also said that they did not have regular interactions with TSA or relied more on the Coast Guard instead for communicating TWIC® information. In addition, four of the same six industry associations said that TSA did not routinely attend their meetings, despite holding a seat on the committee. The other 5 Area Maritime Security Committees either had strong working relationships with TSA staff or did not have issues with their local TSA staff, such as Transportation Surface Inspectors, with whom they interact at the ports.

Delays Receiving Key Program Updates. Three of the six industry associations said they experienced delays in receiving TWIC® program updates from TSA. For example, one of these associations said that a member they represented did not receive official notification from TSA regarding changes to the physical card in 2018 and only discovered this update when their existing TWIC® readers suddenly could not scan the older version of the cards. In addition, TSA told us that in July 2024, a technical issue required the agency to relocate the server address for the Canceled Card List. This meant that users who previously relied on technology integrated with the Canceled Card List such as the card readers would need to update their technology to continue validating TWIC® cards. TSA officials said that they communicated this change to the Coast Guard specifically in January 2024, but stakeholders said that they did not receive this update. As of May 2026, the Coast Guard was in the process of sourcing new readers to conduct security inspections. In the meantime, Coast Guard officials told us that they have been

conducting visual inspections of TWIC cards, since it does not have readers that can integrate with the Canceled Card List.

Standards for Internal Control in the Federal Government states that management should externally communicate quality information necessary for achieving the entity's objectives.²⁹ Specifically, management should communicate with and obtain quality information from external parties, such as contractors and the public, using established reporting lines with open, two-way external reporting. When we spoke with TSA officials, they acknowledged that their lack of a documented communication plan could cause future problems with continuity if there were changes to its workforce. They also noted that a communication plan could be useful for proactively identifying the strategies and tactics for engagement and providing assurance that stakeholders are informed of program updates and other information that affect their operations.

Gaps in how TSA communicates program updates and other information to TWIC® stakeholders, including industry stakeholders, limits stakeholders' ability to prepare for changes. Developing and implementing a communication plan to systematically relay program updates and other information to stakeholders could help TSA reduce security risks.

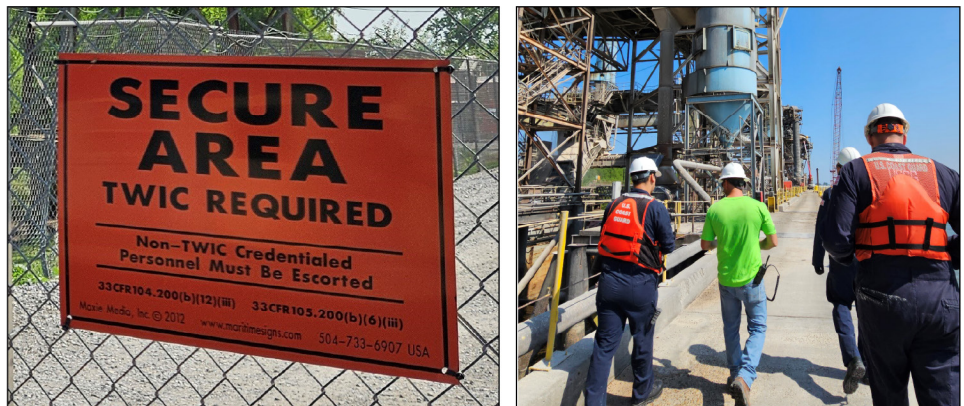
²⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-25-107721](#) (Washington, D.C.: May 15, 2025).

Coast Guard Oversees Facility Operators' Implementation of TWIC® through Inspections but Gaps Exist in Its Processes

Coast Guard Inspects Facilities for Compliance with TWIC® Requirements

The Coast Guard told us that they annually inspected approximately 3,400 MTSA-regulated facilities for regulatory violations and deficiencies, including those related to TWIC®. Figure 4 shows Coast Guard staff inspecting a MTSA-regulated facility.

Figure 4: Coast Guard Inspection of Maritime Transportation Security Act-regulated Facility

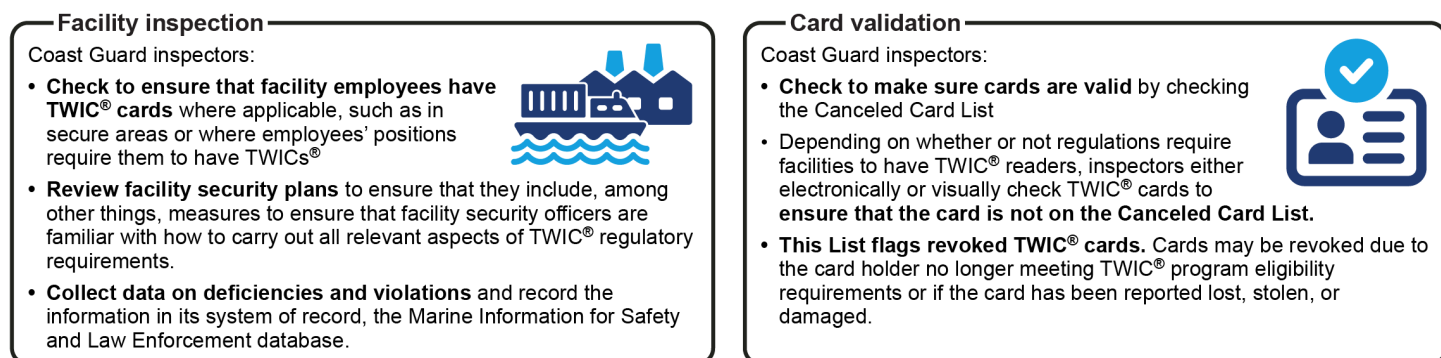


Source: GAO photos. | GAO-26-107521

Note: See Pub. L. No. 107-295, tit. I, § 102(a), 116 Stat. 2064, 2073-74 (2002) (codified as amended at 46 U.S.C. § 70105). For the purposes of this figure, "Maritime Transportation Security Act-Regulated Facilities" are those in 33 C.F.R. § 105.105(a).

To conduct these inspections, the Coast Guard developed a MTSA facility compliance checklist with 179 inspection points for inspectors to review. Of these 179 inspection points, 9 (5 percent) relate to TWIC®, addressing factors such as facility access controls, TWIC® training for security staff and employees, and invalid TWIC® cards, as figure 5 describes.

Figure 5: Coast Guard Transportation Worker Identification Credential (TWIC®)-related Inspection Activities



Source: GAO analysis of Coast Guard documentation. | GAO-26-107521

The Coast Guard defines marine safety deficiencies as any condition, operation, or act pertaining to a vessel or facility that fails to meet acceptable standards. These standards include but are not limited to those established by U.S. laws or regulations, including those involving TWIC® requirements, among other things.³⁰ A more severe form of noncompliance, a violation, including those involving TWIC® requirements, is any deficiency resulting from a failure to meet applicable U.S. statutory or regulatory requirements where sufficient evidence exists to initiate administrative, judicial, or criminal proceedings, as appropriate.³¹ This could involve, for example, a facility operator who does not have a work order to fix a gap in the facility fencing, according to Coast Guard officials.

Coast Guard officials explained that when inspectors encounter a TWIC®-related deficiency, they use discretion to either note the deficiency or issue a notice of violation to the facility operator based on the severity of the deficiency or if it has been a recurring problem.³² For example, regulations require that unescorted workers have TWIC® cards

³⁰United States Coast Guard Commandant, *Marine Safety Manual, Volume I, Administration and Management, COMDTINST M16000.6*. (August 2017).

³¹United States Coast Guard Commandant, *Marine Safety Manual, Volume I, Administration and Management, COMDTINST M16000.6*. (August 2017). See also 33 C.F.R. § 1.07-11 (concerning notices of violation)

³²For the purposes of this report, a "TWIC®-related deficiency" is a deficiency which involves noncompliance with TWIC® related regulations in 33 C.F.R. parts 101 and 105.

when accessing secure areas.³³ However, an inspector may find a worker without a TWIC® card and allow that worker to retrieve their card within 15 minutes, documenting this as a deficiency, instead of issuing a notice of violation for the noncompliance, according to Coast Guard officials. Table 1 describes the most common TWIC®-related deficiencies based on Coast Guard data.

Table 1: Examples of Transportation Worker Identification Credential (TWIC®)-related Deficiencies Cited in 10 Percent or More of U.S. Coast Guard Inspections of Approximately 3,400 Maritime Transportation Security Act-regulated Facilities from Fiscal Years 2019-2024

Coast Guard deficiency description ^a	Deficiency citation	Example	Percentage of total number of deficiencies, fiscal years 2019–2024 ^b
Failure to ensure facility personnel with security duties are qualified to perform specified duties.	33 C.F.R. § 105.210	The facility security guard is not conducting physical screening at random intervals.	26% (227 deficiencies)
Failure to implement facility security measures for access control.	33 C.F.R. § 105.255(a)(4)	Facility failed to prevent an unescorted individual from entering a secure area without a valid TWIC® card.	15% (129 deficiencies)
Failure of facility operator to ensure the facility operates in compliance with security requirements.	33 C.F.R. § 105.200	Personnel without TWIC® cards should have side by side escorting in a secure area. Multiple individuals were observed in secure areas without escorts or TWIC® cards.	10% (92 deficiencies)

Source: GAO analysis of Coast Guard data. | GAO-26-107521

^aSee Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, tit. I, § 102(a), 116 Stat. 2064, 2073-74 (codified as amended at 46 U.S.C. § 70105). For the purposes of this table, “Maritime Transportation Security Act-Regulated Facilities” are those in 33 C.F.R. § 105.105(a).

^bThe Coast Guard found a total of 888 TWIC®-related deficiencies for fiscal years 2019 through 2024.

When the Coast Guard inspectors note a deficiency, they record information about the deficiency in the Coast Guard’s system of record and provide a form to the facility operator explaining the deficiency.³⁴ Inspectors also record violations in the system of record and instead of providing a deficiency form, they issue a notice of violation to the facility

³³See 33 C.F.R. § 105.255(a)(4).

³⁴The Coast Guard’s Marine Information for Safety and Law Enforcement system is designed to capture information required to support the Coast Guard’s marine safety, security, environmental protection, and law enforcement programs.

operator, according to Coast Guard officials.³⁵ The responsible party, such as the facility operator, can either pay the proposed civil penalty or decline the notice of violation and request that the Coast Guard Hearing Office adjudicate the violation.³⁶

Coast Guard Reviews TWIC®-related Violations Data but Does Not Share these Data with Inspectors in the Field

Coast Guard headquarters officials told us that they review TWIC®-related violations data to identify and provide any necessary policy guidance to inspectors in the field but do not provide the data to the inspectors who enforce TWIC® regulatory requirements.³⁷

Since the Coast Guard reviews but does not analyze TWIC®-related violations data at a more granular level, we assessed these data to identify trends for TWIC® noncompliance.³⁸ While the TWIC® items on the inspection checklist comprised just 5 percent of all inspection items, we found that TWIC®-related violations made up 38 percent (83) of the 216 facility inspection violations from fiscal year 2019 through 2024. This magnitude underscores the significance of TWIC® noncompliance as part of overall MTSA-regulated facility security. Figure 6 shows TWIC® violations as a share of all violations by year, with 3 of the 6 fiscal years—2021, 2022, and 2023—showing TWIC®-related violations eclipsing 50 percent of the total number of facility inspection violations. For example, TWIC® violations in fiscal year 2022 were 52 percent of all inspection violations and in fiscal year 2023, they were 53 percent, as shown in figure 6.

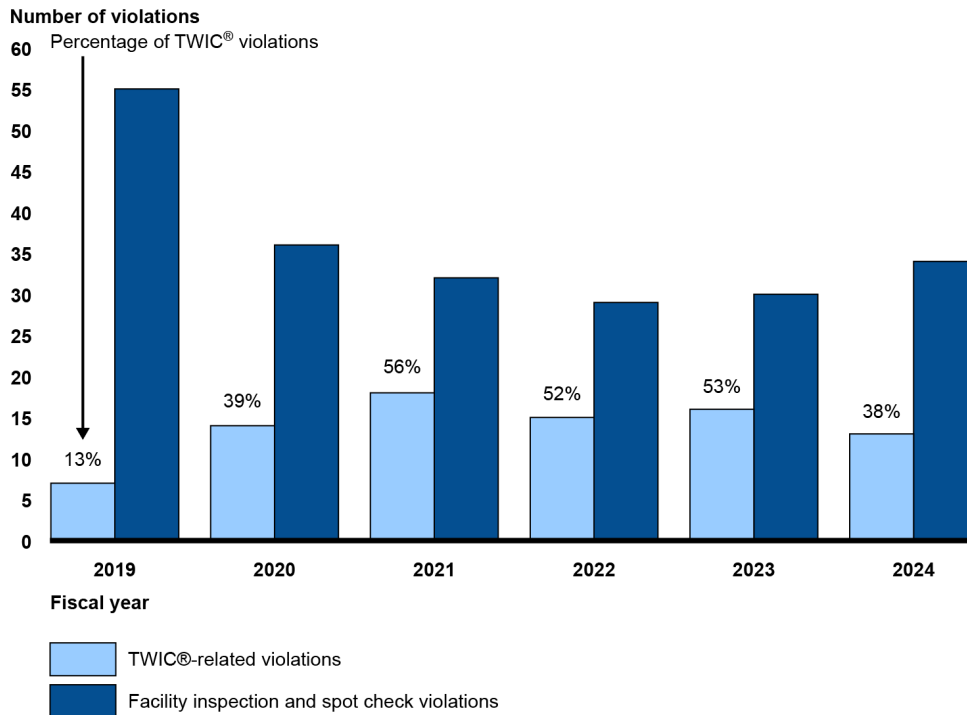
³⁵See 33 C.F.R. § 1.07-11.

³⁶If within 45 days of receipt a party fails to pay the proposed penalty on the Notice of Violation and fails to decline the Notice of Violation, then the Coast Guard will enter a finding of default in the case file and proceed with the civil penalty in the amount recommended on the Notice of Violation without sending it to the Hearing Office. 33 C.F.R. § 1.07-11(f).

³⁷For the purposes of this report, a “TWIC® related violation” is a violation which involves noncompliance with TWIC®-related regulations in 33 C.F.R. parts 101 and 105.

³⁸Coast Guard officials told us that they inspect MTSA-regulated facilities for items beyond the TWIC® regulatory requirements, including MTSA regulations and international guidelines, in addition to ensuring that the facility operator is complying with the facility security plan requirements and using good marine practices.

Figure 6: Transportation Worker Identification Credential (TWIC®)-related Violations as a Share of All Coast Guard Facility Inspection Violations for the Approximately 3,400 MTSA-regulated Facilities, Fiscal Year 2019-2024

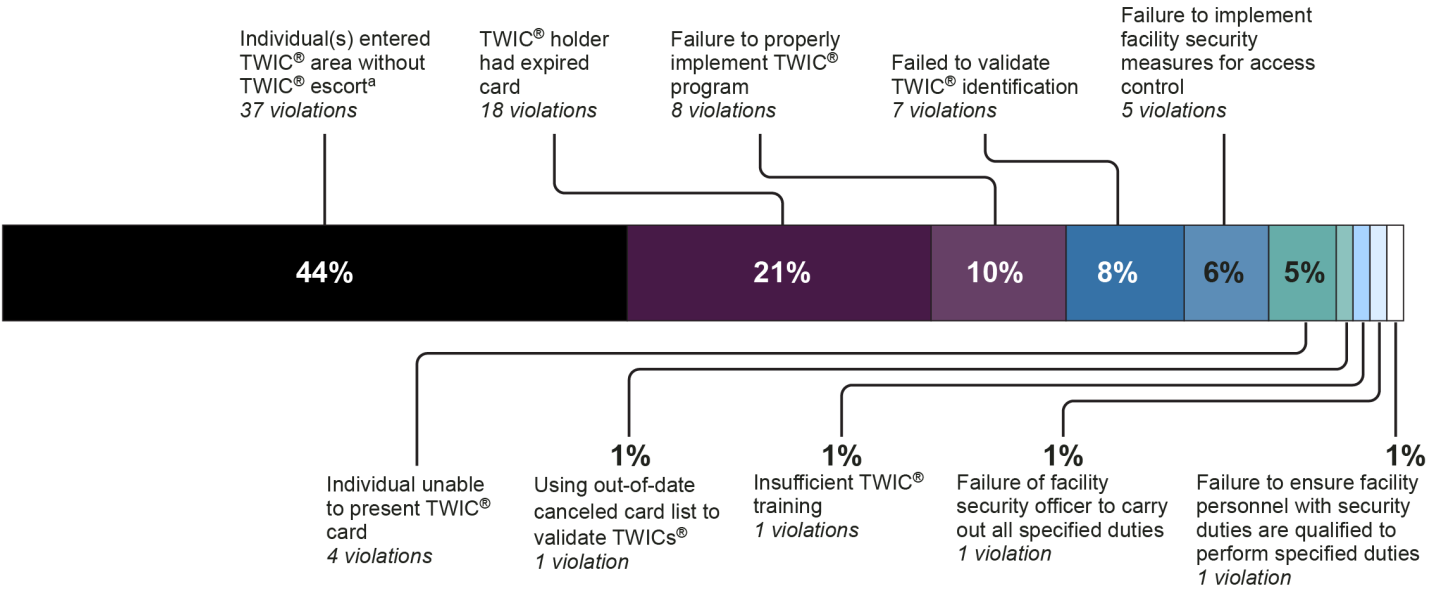


Source: GAO analysis of TWIC® violations data. | GAO-26-107521

Notes: Coast Guard inspectors can issue notices of violations to MTSA-regulated facility operators for both TWIC®-related and non-TWIC®-related violations, such as failing to conduct and record required security drills and exercises and lacking a backup communications system for internal and external communications. For the purposes of this figure, “MTSA-Regulated Facilities” are those in 33 C.F.R. § 105.105(a). Coast Guard officials told us that the comparatively high number of facility inspection and spot check violations for 2019 was likely due to an increased focus on TWIC compliance by the field in preparation for the final TWIC® rule, which at that time, had been anticipated to be implemented in 2020. While initially given an effective date of August 23, 2018, a TWIC reader rule was implemented on June 8, 2020 for certain facilities. See 81 Fed. Reg. 57,652 (Aug. 23, 2016). However, Coast Guard delayed enforcement of this regulation until January 1, 2022, due to the COVID-19 pandemic. 89 Fed. Reg. 86,723 (Oct. 31, 2024).

Our analysis of TWIC®-related violations data also found a prevalence of violations related to unescorted individuals entering a secure area. Figure 7 describes the types of TWIC®-related violations the Coast Guard recorded for fiscal years 2019 through 2024.

Figure 7: Types of Transportation Worker Identification Credential (TWIC®)-related Violations the Coast Guard Recorded for Inspections Conducted, Fiscal Years 2019–2024



Source: GAO analysis of TWIC® violations data. | GAO-26-107521

^aTWIC® escort regulations generally allow individuals without a TWIC® to enter secure areas of maritime facilities when escorted by a valid TWIC® holder. 33 C.F.R. §§ 101.105, 101.515(a), 101.550(d).

Although a less severe form of noncompliance, our analysis of TWIC®-related deficiencies also produced insights on potential TWIC®-related risks, as described later in this report.

Coast Guard headquarters officials told us that they have not communicated TWIC®-related violation and deficiency data to inspectors in the field because they have not identified any TWIC® issues that require a policy change and subsequent notification to inspectors. However, the Coast Guard’s 2020 *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* emphasizes that communication should occur during all phases of enterprise risk management. According to the Framework, communication is critical to risk recognition, awareness of risk appetite and tolerance, identification of response and treatment options, and understanding of management decisions and direction.

By communicating the TWIC®-related violation data that it already collects to inspectors in the field who enforce TWIC®, the Coast Guard

could improve inspectors' awareness and management of TWIC®-related risks.

Coast Guard Uses Data on TWIC®-related Violations but Not Deficiencies to Measure TWIC®-related Enforcement

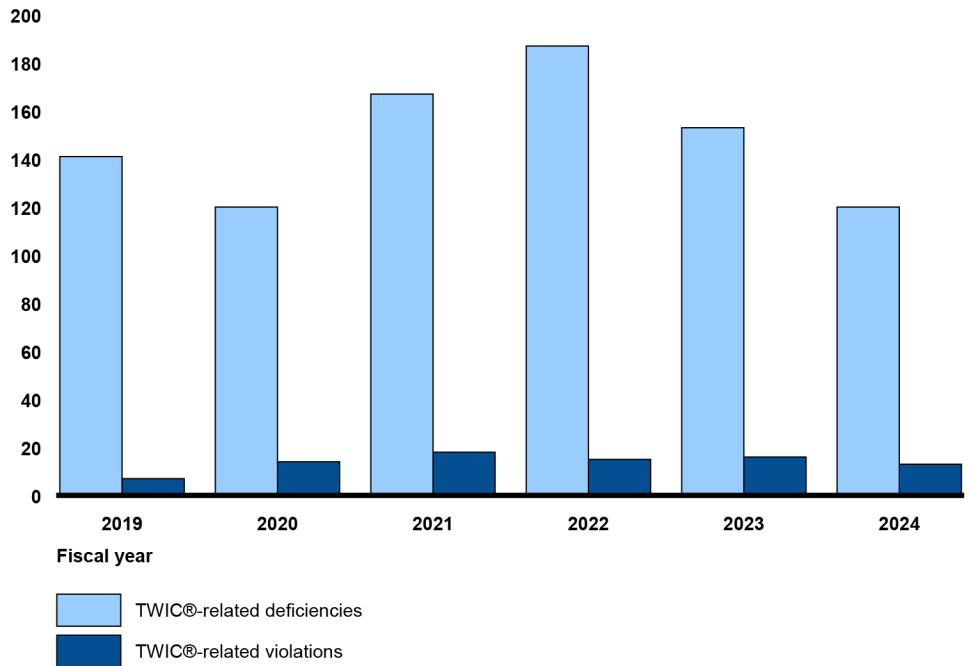
The Coast Guard's performance measure related to the agency's oversight of TWIC® compliance uses data on TWIC®-related violations, but not on deficiencies. Specifically, the Coast Guard's performance measure includes a target of 99 percent compliance with TWIC® regulations. The agency assesses this as the percentage of MTSA-regulated facilities that did not receive a notice of violation or civil penalty for TWIC® noncompliance.³⁹ The Coast Guard reported that at least 99 percent of the approximately 3,400 total MTSA-regulated facilities did not receive a TWIC®-related notice of violation or civil penalty from fiscal year 2019 through 2024. As with the TWIC®-related violations data, Coast Guard officials reported that they do not communicate TWIC®-related deficiency data to inspectors in the field who enforce TWIC® requirements, unless there is a need to provide any necessary TWIC® policy guidance to field inspectors.

However, TWIC®-related deficiencies are also a form of noncompliance, though a less severe form. When we assessed both TWIC®-related violation and deficiency data, we found a more comprehensive description of potential areas of risk for TWIC®-related enforcement. Specifically, Coast Guard inspectors found 83 violations and 888 deficiencies for the TWIC® program across the 3,400 MTSA-regulated facilities from fiscal year 2019 through 2024, as shown in figure 8. This indicates that the percentage of MTSA-regulated facilities complying with TWIC® regulations may be lower than 99 percent.

³⁹For purposes of calculating compliance, the Coast Guard counts facilities, not violations. This means that if a facility has at least one violation, the facility is counted as one facility regardless of whether the number of violations at that facility is one or one hundred.

Figure 8: Total Number of Transportation Worker Identification Credential (TWIC®)-related Deficiencies and Violations for the Approximately 3,400 MTSA-regulated Facilities, Fiscal Years 2019-2024

Number of deficiencies or violations found by Coast Guard inspectors



Source: GAO analysis of TWIC® deficiency and violation data. | GAO-26-107521

Note: For the purposes of this report, a “TWIC®-related deficiency” is a deficiency which involves noncompliance with TWIC® related regulations in 33 C.F.R. parts 101 and 105. A “TWIC®-related violation” for the purposes of this report is a violation which involves noncompliance with TWIC® related regulations in 33 C.F.R. parts 101 and 105. For the purposes of this figure, “MTSA-regulated Facilities” are those in 33 C.F.R. § 105.105(a).

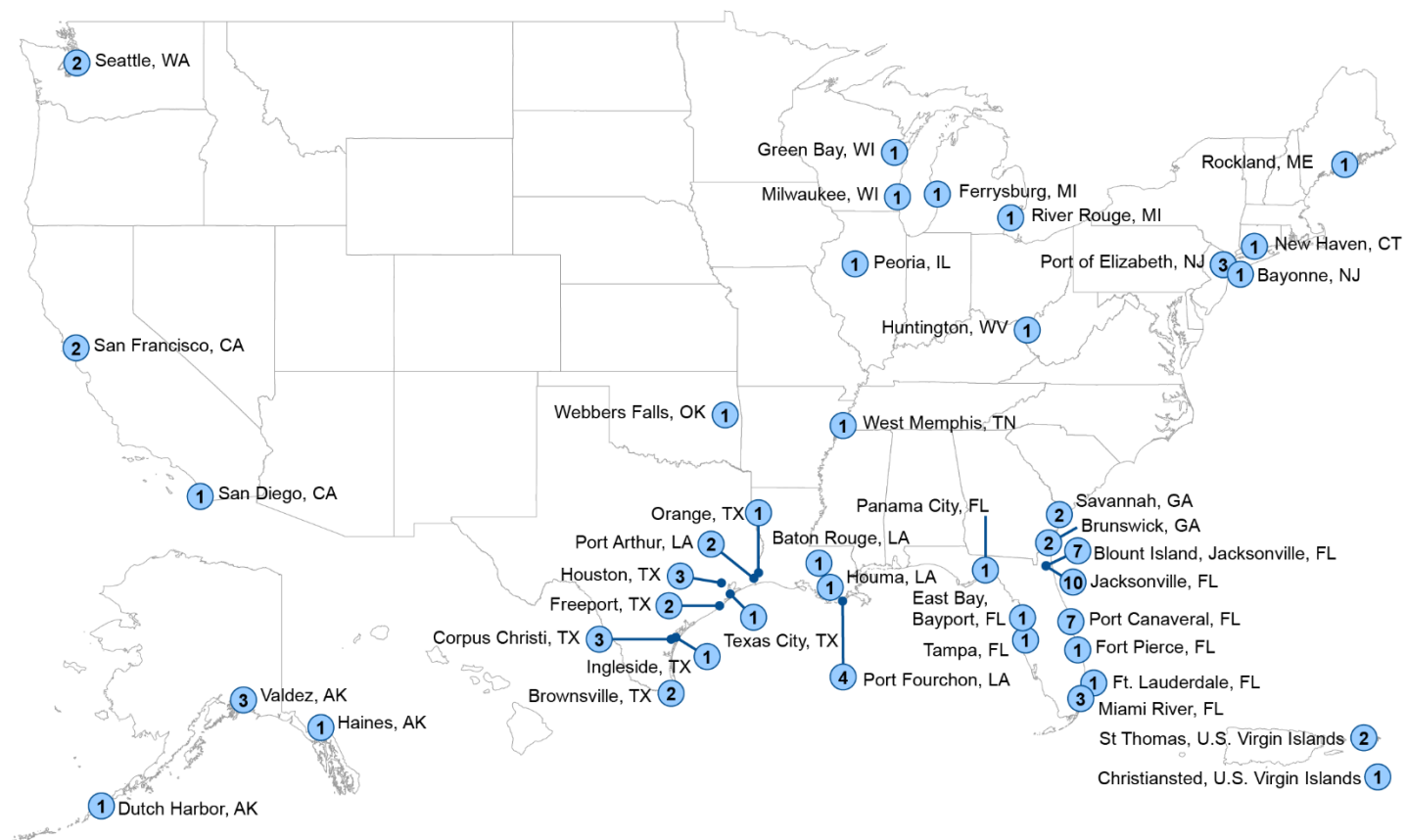
The 83 TWIC®-related violations Coast Guard inspectors cited across the approximate 3,400 MTSA-regulated facilities from fiscal years 2019 through 2024 involved ten types of violations. The 888 TWIC®-related deficiencies involved 41 types. Our analysis showed that the greatest share of all deficiencies—26 percent—were for a failure to ensure that facility personnel with security duties were qualified to perform their roles, such as a facility security guard who did not have a valid TWIC®. The second highest share—approximately 15 percent—was for a failure to prevent an unescorted individual without a TWIC® from entering a secure area.

We also found a more comprehensive description of regional and nationwide TWIC® compliance and potential areas of risk using TWIC®

deficiency data rather than TWIC®-related violations data alone. The highest number of TWIC®-related deficiencies—60—occurred in ports located in the Jacksonville, Florida area followed by Tampa, Florida with 34 deficiencies, according to our analysis. Similarly, we found that the highest number of TWIC®-related violations occurred in Florida, with Jacksonville area ports incurring 10 violations and Cape Canaveral with seven violations, as shown in figure 9. However, TWIC®-related deficiencies were more geographically diffuse as compared to violations. For example, Coast Guard inspectors found deficiencies in an additional 173 ports.⁴⁰

⁴⁰In addition, Coast Guard inspectors found deficiencies in 16 facilities located outside of a port.

Figure 9: Geographic Dispersion of 83 Transportation Worker Identification Credential (TWIC®)-related Violations Coast Guard Recorded for Inspections for the Approximately 3,400 Maritime Transportation Security Act of 2002 (MTSA)-regulated Facilities in Fiscal Years 2019–2024



Source GAO analysis of TWIC® violation data; U.S. Census Bureau (map) | GAO-26-107521

Note: See Pub. L. No. 107-295, tit. I, § 102(a), 116 Stat. 2064, 2073-74 (codified as amended at 46 U.S.C. § 70105). For the purposes of this report, a “TWIC®-related violation” is a violation which involves noncompliance with TWIC®-related regulations in 33 C.F.R. parts 101 and 105. For the purposes of this figure, “MTSA-regulated Facilities” are those in 33 C.F.R. § 105.105(a).

The Coast Guard’s 2020 *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* emphasizes that communication should occur during all phases of enterprise risk management. According to the Framework, communication is critical to risk recognition, awareness of risk appetite and tolerance, identification of response and treatment options, and understanding of management decisions and direction.

The Coast Guard defines deficiencies as less severe forms of noncompliance than violations and, therefore, does not see the need to include deficiency data in its TWIC® performance measure reporting. However, Coast Guard officials told us that they could add deficiency data to the TWIC® performance measure by using the same calculation that they already perform for measuring TWIC®-related violations. Our analysis shows that the Coast Guard's practice of reporting only TWIC®-related violation data does not fully capture its TWIC® enforcement efforts, which include monitoring deficiencies for potential areas of risk. By using deficiency data as well as violations data to measure TWIC® compliance, the Coast Guard could improve its awareness of and response to potential TWIC®-related risks.

Coast Guard Has Not Taken Steps to Mitigate Risks of Individuals on the TWIC® Canceled Card List Accessing Secure Areas of Facilities

The Coast Guard uses TSA's Canceled Card List to mitigate the risk that individuals with revoked TWIC® cards could access secure areas of facilities, but it has not required all facilities to check this list, according to Coast Guard officials. Currently, only high-risk facilities that are required to use TWIC® readers are required to check the Canceled Card List. The remainder of facilities can check the Canceled Card List at their discretion, but there is no requirement that they do so.

TSA places TWIC® cards on the Canceled Card List if

- the agency, upon receiving recurrent vetting flags, rules the TWIC® card holder ineligible due to disqualifying offenses, such as having an arrest warrant; or
- a TWIC® holder reports the card as lost or stolen.

Facility operators can download the Canceled Card List for use with TWIC® readers, or, in the absence of readers, manually consult this list, which is publicly available as a spreadsheet.⁴¹ The TWIC® readers automatically connect to the list which is updated daily. Using the TWIC® readers allows them to flag individuals with revoked TWIC® cards upon entry and prevent them from accessing secure areas of MTSA-regulated facilities. In addition, TSA offers a free iOS and Android application—

⁴¹TSA maintains on its Canceled Card List website the following Canceled Card List formats: a Canceled Card List showing the Federal Agency Smart Credential-Number; a Visual Canceled Card List showing the Credential Identification Number; and integrity hash mark versions of both the Canceled Card List showing the Federal Agency Smart Credential Number and Canceled Card List showing the Credential Identification Number for data reliability purposes.

ADVISR—that allows users, including the public and facility operators, to scan the TWIC® card’s barcode to determine if it is on the list.

Checking the Canceled Card List for facilities required to use TWIC® readers. Regulations currently only require facilities that receive vessels certificated to carry 1,000 or more passengers (e.g., cruise ship terminal operators) to use TWIC® card readers but does not require other types of facilities to use them. Because of this requirement, the Coast Guard monitors for the use of card readers while inspecting cruise terminal facilities. Additionally, Coast Guard officials said that they have an ongoing process to reevaluate other types of high-risk facilities, such as those that handle Certain Dangerous Cargoes in bulk, to determine if they will eventually require them to use readers, which we discuss later in this report.

While officials from eight of the 10 Area Maritime Security Committees we spoke with had readers at some or all of the facilities in their respective ports, officials from the other two committees reported that readers are not in use at any of their facilities. According to officials from one committee, this was largely due to functionality concerns and the costs of implementing the readers. An Area Maritime Security Committee official representing the cruise ship industry reported that his organization spent 10 percent of their \$400,000 security budget on upgrading the TWIC® readers. Additionally, officials from one Area Maritime Security Committee we spoke with reported that smaller facilities do not have the capacity to spend 25 percent of their budget on implementing the TWIC® readers.

Checking the Canceled Card List for facilities not required to use TWIC® readers. Officials from one committee explained that if security staff at facilities without TWIC® readers want to manually search the Canceled Card List’s online spreadsheet, they must match the eight-digit number on each TWIC® card to those numbers listed on the spreadsheet. According to committee members, this can be subject to error. Officials from one committee noted that facility security staff often do not use the manual list to validate TWIC® cards. In addition, none of the officials across the 10 committees we interviewed reported using the ADVISR application to validate cards. As a result, security staff at facilities without TWIC® readers may not be manually checking the Canceled Card List to identify revoked TWIC® cards. For example:

Officials from one committee explained that, unless their facilities had readers linked to the Canceled Card List, they would not know if an employee’s card had been revoked. As such, the TWIC® card holder’s

employer or facility operators would be unaware that this employee is accessing secure areas of MTSA-regulated facilities with a revoked TWIC® card.

Officials from another committee told us that a worker used his father's TWIC® card because his card was on the Canceled Card List and the facility did not have a reader to flag the card.

Coast Guard officials reported that while they do not require facility operators to check the Canceled Card List manually, they do encourage the practice to prevent unescorted access by individuals without a valid TWIC®. These officials acknowledged that unauthorized access is a potential risk to the security of other facilities not currently required to have card readers or to manually check the Canceled Card List. However, Coast Guard officials said that they have not developed a method for mitigating this risk because the TWIC® regulatory requirements do not require facility operators to manually check the Canceled Card List. To require this for other MTSA-regulated facilities, Coast Guard officials stated that the agency would need to promulgate a new regulation.

The Coast Guard's current lack of regulatory requirements for facility operators without readers to manually check the Canceled Card List does not preclude the Coast Guard from developing a method to mitigate the risk of individuals with canceled cards obtaining access to secure areas, which could include promulgating a regulatory requirement or making recommendations to operators. Further, the Coast Guard, by not addressing the risk raised by facility operators not checking the Canceled Card List, leaves some high-risk facilities without cruise ship terminals vulnerable to unauthorized individuals accessing secure spaces.

The Coast Guard's 2020 *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* states that risk treatment is the process of selecting and implementing measures to modify specific risks. These include controls to limit or reduce the likelihood of risk events or to mitigate their impact if they do occur.⁴² The Framework advises that preventive controls are designed to limit the possibility of an undesirable outcome and can include oversight activities

⁴²United States Coast Guard, *Framework for Strategic Mission Management*.

to ensure the organization properly implements the controls and achieves the relevant objectives for reducing risk.

Without a method to mitigate the risk of individuals on the Canceled Card List accessing secure areas of all MTSA-regulated facilities, the Coast Guard's preventive controls are limited. Developing such a method would help restrict the access of unauthorized individuals and help ensure controlled areas remain secure.

Coast Guard and TSA Have Not Coordinated Their Acquisition of Inspection Devices to Validate TWIC® Cards

The Coast Guard and TSA are in the process of acquiring new devices for validating TWIC® cards during their respective inspections, but they have not coordinated their efforts. Specifically, though TSA and the Coast Guard are both DHS components, they have each used separate, fragmented approaches rather than department-wide procurement processes for acquiring the new devices.⁴³

Coast Guard. The Coast Guard terminated its 2022 contract for devices—handheld readers—in September 2024, after a server update rendered the readers obsolete. Coast Guard officials reported that since the server update inspectors have been conducting visual inspections of TWIC® cards. Figure 10 shows a servicemember verifying a TWIC® by hand as well as the legacy handheld TWIC® reader.

⁴³Fragmentation occurs when more than one agency (or more than one organization within an agency) is involved in the same broad area of national need. GAO, *Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve an Additional One Hundred Billion Dollars or More in Future Financial Benefits*, [GAO-25-107604](#) (May 13, 2025).

Figure 10: Coast Guard Servicemember Verifies Transportation Worker Identification Credential (TWIC®) Manually; Legacy Coast Guard TWIC® Reader



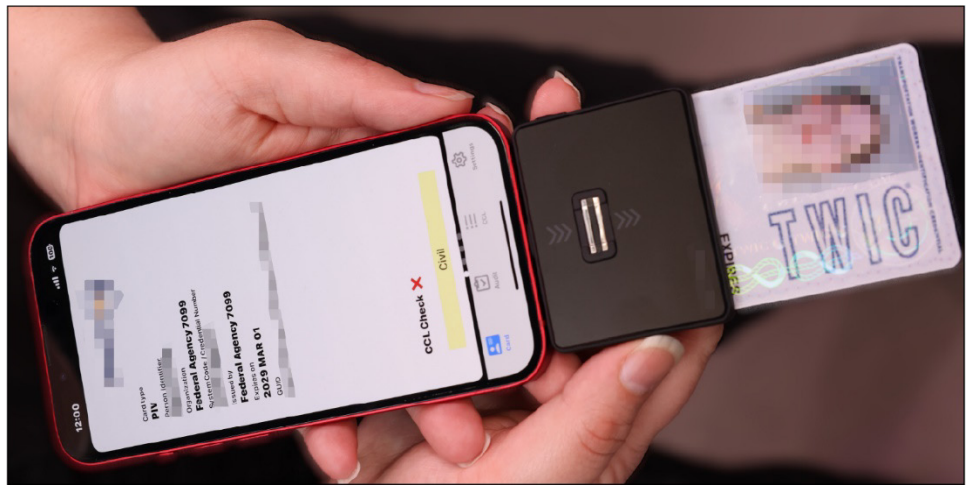
Source: GAO photos. | GAO-26-107521

In September 2025, the Coast Guard awarded a contract for \$1.4 million to procure 250 handheld readers, but the contract was terminated due to a protest of the contract and lapse in appropriations, according to the Coast Guard. Coast Guard officials told us in May 2026 that the agency is actively pursuing the acquisition of handheld readers and hopes to deliver the readers to inspectors by the end of fiscal year 2026.

TSA. TSA currently uses a smart phone app with an attachment that plugs into a government-issued phone as its device for validating TWIC® cards. However, according to TSA officials, the application and

attachment are incompatible with newer model phones that TSA has been disseminating to inspector staff. Figure 11 shows the TWIC® reader device TSA inspectors attach to their smart phones.

Figure 11: Transportation Security Administration (TSA) Inspector Smart Phone and Associated Plug-In Transportation Worker Identification Credential (TWIC®) Card Reader Device



Source: Transportation Security Administration (TSA) photo. | GAO-26-107521

TSA officials stated that they are early in the acquisition process and expect to acquire handheld readers, like the Coast Guard. TSA officials also stated that it would be ideal if their device requirements could mirror the Coast Guard's requirements. TSA has over 300 licenses for the application it currently uses to read TWIC® cards, but officials have not yet determined the number of handheld readers they would need to replace the current technology.

Officials from both TSA and Coast Guard stated that they could lower the per unit cost of each reader if they coordinated requirements. Coast Guard officials said that since their acquisition effort is underway and coordination efforts will take time, they likely would continue a dual acquisition track. In other words, they would pursue what is already in motion while also exploring options to coordinate with TSA in the future. By doing so, the Coast Guard would likely procure 125 handheld readers the first year of the contract and include option years but not exercise them. This would then allow the Coast Guard to coordinate future procurements with TSA, according to Coast Guard officials. DHS's Office

of the Chief Procurement Officer, Coast Guard, and TSA officials told us they had not previously considered coordinating the acquisition of TWIC® card readers. According to Coast Guard and TSA officials, they had previous user requirements that were not compatible. For example, the Coast Guard had required a level of durability that a phone could not provide.

Coast Guard and TSA officials stated that it takes additional effort to coordinate acquisitions across DHS components, but they noted that the lower contracting efforts and price per unit would outweigh the costs. Specifically, they anticipate possibly reducing contracting efforts and potentially lowering prices per unit but said that it is too early to quantify the impact.

According to DHS's Homeland Security Acquisition Manual and DHS officials, coordination across DHS components would require DHS's Office of the Chief Procurement Officer to be involved.⁴⁴ The manual also states that components are to coordinate with DHS for similar goods and services. Officials from DHS's Office of the Chief Procurement Officer stated that coordination across components is consistent with DHS's goal of centralizing acquisitions. They also cited other executive branch directives which underscore the importance of consolidating procurement efforts.⁴⁵

Additionally, our prior work on collaboration also demonstrates benefits of coordinating on crosscutting challenges or opportunities, which would include the acquisition of TWIC® card readers. For example, collaborating agencies must successfully leverage staffing, funding, and technological resources. In so doing, the agencies would be better able to use each other's assets, thus gaining additional benefits that would be unavailable if they were working separately.⁴⁶

⁴⁴Department of Homeland Security, *Homeland Security Acquisition Manual, Subchapter 3017.70 Intra-Agency Acquisitions and Subchapter 3007.2 Planning for the Purchase of Supplies in Economic Quantities* (Oct. 2009).

⁴⁵*Eliminating Waste and Saving Taxpayer Dollars by Consolidating Procurement*, Exec. Order 14,240, 90 Fed. Reg. 13,671 (Mar. 20, 2025); Office of Management and Budget, *Memorandum to the Heads of Executive Departments and Agencies: Consolidating Federal Procurement Activities*, M-25-31 (July 18, 2025).

⁴⁶GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington D.C.: May 24, 2023).

According to DHS procurement officials, there is an existing DHS-wide identity, credential, and access management contracting vehicle that the Coast Guard and TSA might be able to use for the acquisition of TWIC® card readers.⁴⁷ DHS procurement officials said their early exploration indicates this vehicle may be a good fit. However, they also said they would need more time to formally assess the feasibility of implementing this or a new department-wide contract vehicle—and consider this effort along with existing demands from other components seeking DHS’s procurement support. According to these same officials, part of assessing the feasibility would include assessing the complexity of the acquisition, the similarity of the components’ requirements, the possible benefits to DHS and its components, and the workload of DHS acquisition staff. DHS officials also said the first step in the coordination process would be for Coast Guard and TSA officials to reach out to DHS’s Office of the Chief Procurement Officer.

Coordination among the Coast Guard and TSA to acquire TWIC® reader devices, through DHS’s existing acquisition vehicle or the most appropriate strategic sourcing vehicle available, would streamline currently fragmented processes. Further, it could lead to dollars saved or costs averted for both TSA and the Coast Guard in two key areas:

- reducing labor costs (time and personnel) associated with each component developing the specific requirements, reviewing bids from prospective vendors, and overseeing the quality of the deliverable/monitoring for contractor performance.
- reducing the unit cost of the devices used to check TWIC® cards for validity.

As a result, improved coordination would help ensure that TSA and the Coast Guard are efficiently using taxpayer dollars to help secure the nation’s maritime transportation system.

⁴⁷DHS implemented the identity, credential, and access management contracting vehicle—a blanket purchase agreement—in 2021.

Coast Guard Does Not Have a Plan for Finalizing Which Facilities Must Have TWIC® Biometric Card Readers

Coast Guard Delayed Facilities' Implementation of TWIC® Reader Rules Several Times Since 2009

The SAFE Port Act requires DHS to promulgate final regulations requiring the deployment of TWIC® readers.⁴⁸ For more than 15 years—since 2009—the Coast Guard has promulgated proposed rules and regulations defining if and under what circumstances MTSA-regulated facility operators are to implement TWIC® readers to validate TWIC® cards. However, over that timeframe the Coast Guard has delayed elements of the TWIC® reader implementation four times and delayed the reader rule for full implementation twice. For example, in 2016, the Coast Guard issued a regulation which, among other things, required facilities that receive vessels certificated to carry more than 1,000 passengers, such as cruise ship passenger terminals, to implement TWIC® readers for validating TWIC® cards. While initially given an effective date of August 23, 2018, the 2016 TWIC reader final rule was implemented on June 8, 2020 for certain facilities.⁴⁹ However, Coast Guard officials reported that it delayed enforcement of this regulation until January 1, 2022, due to the COVID-19 pandemic.⁵⁰

The Coast Guard had planned to implement a similar requirement for other facilities, but this has also been delayed. The Coast Guard delayed

⁴⁸The SAFE Port Act amended 46 U.S.C. § 70105 to require the Secretary of the department in which the Coast Guard is operating to enact a card reader pilot program and promulgate final regulations requiring the deployment of card readers consistent with the finding of the pilot program within two years of initiating the pilot program and that build upon regulations to prevent an individual from entering an area of a facility that is designated as a secure area by the Secretary for purposes of an approved security plan for the facility. Pub. L. No. 109-347, § 104, 120 Stat. at 1889-90 (codified at 46 U.S.C. § 70105(j)(3)); see 46 U.S.C. § 70105(a)(1).

⁴⁹See Pub. L. No. 115-230, § 2, 132 Stat. 1631 (2018); 81 Fed. Reg. 57,652 (Aug. 23, 2016); 85 Fed. Reg. 13,493 (Mar. 9, 2020).

⁵⁰See 89 Fed. Reg. 86,723 (Oct. 31, 2024).

the date for required implementation of the TWIC® readers from 2018 to 2029 for facilities that

- handle Certain Dangerous Cargoes in bulk and transfer these cargoes from or to a vessel,
- handle Certain Dangerous Cargoes in bulk but do not transfer them from or to a vessel, and
- receive vessels carrying Certain Dangerous Cargoes in bulk but do not transfer them from or to the vessel during the vessel-to-facility interface.⁵¹

See Appendix V for additional information on the Coast Guard's proposed and final rules, laws, and GAO recommendations for implementing the TWIC® readers.

The Coast Guard attributes many of these delays to concerns stakeholders, such as facility operators, industry organizations, and a labor union have raised regarding how the Coast Guard identified MTSA-regulated high-risk facilities that would be required to implement the TWIC® readers and logistical issues around implementation. For example, stakeholders expressed concerns with how the Coast Guard defined and identified high-risk facilities as well as challenges accessing needed reader technology. GAO and Congress also raised concerns with the Coast Guard's implementation of the TWIC® readers. In 2013, we found that the TWIC® card reader pilot results were unreliable, and that the program's benefits needed to be reassessed.⁵² We recommended that Congress direct DHS to assess the effectiveness of TWIC® card readers and develop a final regulation on them based on the assessment. In response to this report, the explanatory statement accompanying the

⁵¹83 Fed. Reg. 29,067 (June 22, 2018) (proposing delay until August 2021 for two of the three facility categories above); 85 Fed. Reg. 13,493 (Mar. 9, 2020) (delaying the effective date for all three facility categories until May 2023); 87 Fed. Reg. 74,563 (Dec. 6, 2022) (proposing further delay until May 2026); 88 Fed. Reg. 23,349 (Apr. 17, 2023) (amending implementation date to May 8, 2026 to conform with recently passed legislation); 89 Fed. Reg. 86,723 (Oct. 31, 2024) (delaying effective date until May 2029).

⁵²GAO, *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, [GAO-13-198](#) (Washington D.C.: May 8, 2013).

Consolidated Appropriations Act, 2014 directed DHS to complete the recommended assessment by April 17, 2014.⁵³

During the course of our review, officials from eight of the 10 Area Maritime Security Committees we spoke with also identified concerns with implementing the TWIC® readers.

- **Costs:** Officials from eight of the 10 committees we interviewed reported that the cost of implementing the TWIC® readers was a concern. For example, officials from one committee said that they spent \$500,000 to replace more than 100 TWIC® readers after their previous readers became obsolete due to TSA changing how the readers download the Canceled Card List. Officials from the other two committees said the cost was not prohibitive, or did not comment on cost at all.
- **Complexity:** Officials from seven of the 10 committees stated that integrating the TWIC® readers with their facilities' security protocols can be complicated. Officials from the other three committees did not report any concerns with the complexity of implementing TWIC® readers.
- **Functionality:** Officials from seven of the 10 committees explained that the TWIC® readers they have purchased and installed do not consistently work. For example, the TWIC® readers cannot always read the fingerprints of facility workers, who often have dirty or unreadable fingerprints due to chemicals they work with. Officials from the other three committees did not raise any functionality concerns with the TWIC® readers.
- **Operational effects:** Officials from eight of the 10 committees said the time it takes for the TWIC® readers to complete the scanning of the TWIC® card can cause delays in workers accessing facilities, which negatively affects business operations. According to officials from four of these committees, ports with TWIC® readers may experience slower turn-around times, potentially affecting the efficiency and attractiveness of the port for shippers for whom speed is a priority. Officials from the other two committees did not report any operational concerns with the readers.

⁵³160 Cong. Rec. H475, H927 (daily ed. Jan. 15, 2014) (accompanying Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5). The Coast Guard commissioned a 2022 study providing a risk-informed analysis to support the implementation of the final reader rule.

Coast Guard Has Identified Options for Addressing Stakeholder Concerns but Does Not Have a Plan for Finalizing Which Facilities Must Have TWIC® Readers

The Coast Guard has taken steps to address stakeholder concerns by conducting a risk analysis for which types of facilities it will require to implement TWIC® readers. However, it has not developed a plan on how it will issue final regulations to specify which facilities must have TWIC® card readers. In 2020, it commissioned a study of its risk-informed approach to identify facilities that would be subject to the reader rules. RAND issued this study in 2022.⁵⁴ This study found deficiencies in how the Coast Guard was defining facilities that handle Certain Dangerous Cargoes in bulk as well as data collection challenges for accurately identifying these facilities. Specifically, RAND found that many of the facilities that Coast Guard categorized as not handling Certain Dangerous Cargoes reported having these cargoes in other data sources.

This study's authors also explored alternative risk models and sources for data collection that they eventually recommended for the Coast Guard to use. Namely, they suggested a facility risk model based on DHS's Cybersecurity and Infrastructure Security Agency's former Chemical Facility Anti-Terrorism Standards (CFATS) risk engine.⁵⁵

Coast Guard officials told us in March 2025 that in response to the study's results, they began exploring the adoption of the CFATS risk engine and using the Chemical Security Assessment Tool for its TWIC® reader risk analysis. Coast Guard officials reported that they attempted a pilot program for using the risk engine for the TWIC® reader risk analysis but were unable to conduct the pilot due to the expiration of the CFATS statutory authority and loss of CFATS personnel. Coast Guard officials said that following the expiration of the CFATS statutory authority, the agency explored using existing available data and capabilities to perform the TWIC® reader risk analysis. However, they determined that this was not feasible going forward.

Coast Guard officials told us in April 2026 that they are continuing to review options to revise the applicability of the TWIC® reader regulations,

⁵⁴RAND's Homeland Security Operational Analysis Center, *Risk-Informed Analysis of Transportation Worker Identification Credential Reader Requirements* (Santa Monica, California.: 2022).

⁵⁵The CFATS program formerly identified and regulated high-risk facilities to ensure security measures were in place to reduce the risk that certain dangerous chemicals are weaponized by terrorists. Under CFATS, certain facilities were required to report their chemicals to the Cybersecurity and Infrastructure Security Agency via an online survey, which was used to determine if the facility was considered high-risk and were required to develop a security plan. The statutory authority for the CFATS program expired in July 2023.

including determining how to move forward with a proposed rule to identify which facilities should be required to have TWIC® readers. However, they do not have a detailed plan for finalizing this effort, including objectives or time frames. The Coast Guard's *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* states that plan-making is a component of mission management.⁵⁶ Specifically, the Framework states that plan-making should identify and develop feasible ways and means for achieving established priorities and objectives as well as the rationale and justification for adoption. Conceptual planning, according to the Framework, produces viable nascent strategies; detailed planning translates conceptual strategies into complete and practical plans, including implementation specifics.

By not developing and implementing a plan that includes objectives and timeframes describing how it will promulgate the TWIC® reader rules for finalizing which facilities must have TWIC® card readers, the Coast Guard risks additional delays that could leave secure areas of facilities that handle dangerous cargo, like liquified natural gas port terminals, at a greater risk of security breaches.

Conclusions

The TWIC® program's vetting of workers who access secure areas of U.S. maritime facilities helps mitigate the risk of terrorism and other crime at U.S. ports, waterways, and vessels that are critical to maintaining the U.S. economy and global supply chain. However, gaps in how TSA communicates updates to TWIC® stakeholders, including industry stakeholders, limits stakeholders' ability to prepare for updates and program changes. Developing and implementing a communication plan to systematically relay information to stakeholders could help TSA reduce security risks.

Coast Guard officials told us that they do not communicate TWIC®-related violation and deficiency data to inspectors in the field who enforce TWIC® requirements. Communicating these data that it already collects with inspectors in the field could help the Coast Guard improve inspectors' awareness and management of TWIC®-related risks. Additionally, the Coast Guard focuses its assessment of TWIC® enforcement efforts only on the most severe forms of noncompliance—those that resulted in a TWIC®-related notice of violation or civil penalty. By using deficiency data to measure TWIC® compliance more broadly,

⁵⁶United States Coast Guard, *Framework for Strategic Mission Management*.

the Coast Guard could more fully capture its TWIC® enforcement efforts as well as improve its monitoring of potential areas of risk.

In addition, TSA and the Coast Guard have opportunities for enhanced coordination to acquire a single type of device to check the validity of TWIC® cards during inspections. Coordinating the acquisition of these devices could lead to dollars saved or costs averted. It would also reduce fragmentation and help ensure that TSA and the Coast Guard are efficiently using taxpayer dollars to help secure the nation's maritime transportation system.

Facility operators manually checking the Canceled Card List without the benefit of TWIC® biometric card readers can pose an unintentional risk to facility security due to the impracticality of checking every TWIC® card number against a spreadsheet. Developing a method to mitigate risks with the Canceled Card List would help the Coast Guard prevent bad actors from potentially accessing secure areas of MTSA-regulated facilities. Additionally, by not developing and implementing a plan that includes objectives and timeframes describing how it will issue final regulations to specify which facilities must have TWIC® card readers, the Coast Guard risks additional delays in fully meeting the requirements of the SAFE Port Act. These delays could leave facilities that handle dangerous cargo, like liquified natural gas port terminals, at a greater risk of security breaches.

Recommendations for Executive Action

We are making a total of seven recommendations, including two to TSA and five to the Coast Guard. Specifically:

The TSA Administrator should develop and implement a communication plan to systematically relay TWIC® program updates to stakeholders. (Recommendation 1)

The Commandant of the Coast Guard should communicate TWIC®-related violation and deficiency data with inspectors in the field who enforce TWIC® requirements. (Recommendation 2)

The Commandant of the Coast Guard should include deficiency data in its TWIC® performance measure reporting. (Recommendation 3)

The Commandant of the Coast Guard should develop a method to mitigate the risks of unauthorized individuals with TWIC® cards on the Canceled Card List accessing secure areas of MTSA-regulated facilities. (Recommendation 4)

The Commandant of the Coast Guard should coordinate with TSA, through DHS, to acquire TWIC® reader devices for use during inspections. (Recommendation 5)

The TSA Administrator should coordinate with the Coast Guard, through DHS, to acquire TWIC® readers for use during inspections, as appropriate. (Recommendation 6)

The Commandant of the Coast Guard should develop and implement a plan on how it will issue final regulations to specify which facilities must have TWIC® card readers. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and the Department of Justice for review and comment. In its comments, reproduced in appendix VI, DHS agreed with all seven of our recommendations. DHS and the Department of Justice also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at ShermanT@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VIII.

//SIGNED//

Tina Won Sherman
Director, Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This report examines the following:

1. The extent to which TSA has communicated Transportation Worker Identification Credential (TWIC®) program information to stakeholders.
2. The extent to which the Coast Guard has overseen the implementation of the TWIC® program by facility operators.
3. The extent to which TSA and the Coast Guard have coordinated to acquire devices for purposes of inspecting TWIC® cards for validity.
4. The implementation status of TWIC® biometric card readers.

To address how the Transportation Security Administration (TSA) has effectively communicated with stakeholders, particularly any program changes, we interviewed TSA officials from the Enrollment Services and Vetting program, who oversee applicant services, and from the Office of Intelligence and Analysis, who oversee screening. We also reviewed evidence these officials provided to document these changes, such as a technical advisory regarding a change to the program operations.

In addition, we interviewed industry representatives from six organizations whose members hold a TWIC® to discuss their views on how effectively TSA communicates TWIC® program updates with them. We chose these industry organizations in part based on the type of membership and history of providing feedback to Congress, TSA, and the Coast Guard. We also obtained perspectives on TSA's stakeholder communication from members of a nongeneralizable sample of 10 Area Maritime Security Committees.¹ We selected this sample from a total of 57 committees based on several factors, including for their larger size and wider range of port operations, high volume of TWIC® enrollments for committee-adjacent enrollment centers, and the committee's geographic coverage. Lastly, we reviewed and assessed TSA's communication practices

¹The Maritime Transportation Security Act of 2002 (MTSA) provided for the establishment of Area Maritime Security Committees. Pub. L. No. 107-295, tit. I § 102(a), 116 Stat. 2064, 2081 (codified as amended at 46 U.S.C. § 70112). These committees provide a link for contingency planning, development, review, and update of Area Maritime Security Plans and to enhance communication between port stakeholders within federal, state and local agencies, and industry to address maritime security issues. The 10 committees we selected and contacted included private industry members, such as facility security officers, first responders, Coast Guard sector personnel, and TSA surface inspectors.

against GAO's Standards for Internal Control, which set forth best practices for communication with external stakeholders.²

To understand how the Coast Guard oversees facility operators' compliance with TWIC® regulatory requirements and mitigates any TWIC®-related risks, we analyzed TWIC®-related deficiency and violation results from the Coast Guard's Maritime Transportation Security Act (MTSA)-regulated facility inspections.³ Specifically, we analyzed the results for fiscal years 2019 through 2024 to identify the most prevalent forms of noncompliance. We also compared the total number of the Coast Guard's MTSA-regulated facility violations to the number of TWIC®-related violations to determine the magnitude of TWIC®-related violations as a share of the total.⁴ To assess the reliability of the TWIC®-related deficiencies and violations data, we reviewed documentation such as the user guide for the Coast Guard's system of record, the Marine Information for Safety and Law Enforcement database. We also interviewed Coast Guard officials regarding how they inspect for TWIC®-related violations and deficiencies and use these data to help inform enforcement, as well as what quality assurance controls are in place for ensuring the reliability of these data. We determined these data to be sufficiently reliable for reporting on TWIC® noncompliance trends over the six-year period. To analyze how the Coast Guard mitigates the risk that individuals with revoked TWIC® cards could access secure areas of facilities, we reviewed Coast Guard guidance and regulations on the Canceled Card List. We also interviewed Coast Guard officials and members from the 10

²GAO, *Standards for Internal Control in the Federal Government*, [GAO-25-107721](#) (Washington, D.C.: May 15, 2025).

³For the purposes of this report, "MTSA-regulated facilities" are those which are subject to 33 C.F.R. part 105. 33 C.F.R. § 105.105(a). Coast Guard inspectors can issue violations for instances in which a MTSA-regulated facility operator has not complied with TWIC® regulatory requirements, such as for expired TWIC® cards or individuals entering secure facility areas without a TWIC® escort. Under Coast Guard policy, deficiencies are a less severe form of noncompliance with regulatory requirements.

⁴The Coast Guard defines marine safety deficiencies as any condition, operation, or act pertaining to a vessel or facility that fails to meet acceptable standards. These standards include but are not limited to those established by U.S. laws or regulations, including those involving TWIC® requirements, among other things. A more severe form of noncompliance, a violation, including those involving TWIC® requirements, is any deficiency resulting from a failure to meet applicable U.S. statutory or regulatory requirements where sufficient evidence exists to initiate administrative, judicial, or criminal proceedings, as appropriate.

previously described Area Maritime Security Committees on how facility operators use this list to guard access to secure areas.

We also visited a port with MTSA-regulated facilities, selected due to its large commodity volume and risk level to interview Coast Guard inspectors and observe a Coast Guard inspection of MTSA-regulated facility for TWIC® compliance. We interviewed (1) Coast Guard officials who oversee inspections and (2) industry stakeholders as identified above regarding their perspectives on the implementation of TWIC® requirements. Using the totality of this information, we compared the Coast Guard's TWIC® enforcement efforts and outcomes against its *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* to assess how it measures TWIC® compliance and addresses risk.⁵

To assess the extent to which TSA and the Coast Guard have coordinated to acquire devices for purposes of inspecting TWIC® cards for validity, we reviewed each component's available acquisition documentation. This included the 2018 TSA and 2024 Coast Guard statements of work for purchased services. We also interviewed TSA and Coast Guard contracting officials to better understand the requirements each component had for inspectors' use of these devices in the field, the history of their acquisitions, past and planned expenditures to acquire devices, and any obstacles and benefits to coordination. In addition, we interviewed Department of Homeland Security (DHS) officials from the Office of the Chief Procurement Officer to understand their role in facilitating collaborative acquisition efforts within the department and their processes for doing so.

To address the status of TWIC® reader implementation across MTSA-regulated facilities, we reviewed TWIC® biometric card reader requirements in the SAFE Port Act, the Coast Guard's proposed and issued regulations, and related Coast Guard documentation from 2006 through 2025, which included the year DHS was first required to conduct a TWIC® reader program.⁶ We also synthesized written comments

⁵United States Coast Guard Deputy Commandant for Operations, *Framework for Strategic Mission Management, Enterprise Risk Stewardship, and Internal Control* (July 2020).

⁶The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) required the Secretary of the department in which the Coast Guard was operating to conduct a TWIC® reader pilot program and promulgate within 2 years of initiating this program the final regulations requiring the deployment of TWIC® readers. Pub. L. No. 109-347, tit. I, § 104, 120 Stat. 1884, 1889-90. For more information, see table 3 and appendix V.

submitted by TWIC® stakeholders, such as facility operators and industry associations, in response to the Coast Guard's proposed TWIC® reader rules to identify concerns with TWIC® reader implementation. Additionally, we reviewed RAND's 2022 report assessing the Coast Guard's TWIC® reader risk analysis and interviewed the report authors and other RAND subject matter experts about the TWIC® reader implementation.⁷

To identify and assess the steps the Coast Guard is taking to address stakeholder concerns with the TWIC® reader risk analysis, we interviewed Coast Guard officials from the Office of Port and Facility Compliance who are responsible for the risk analysis and promulgating the TWIC® reader rules. In addition, we interviewed officials from the 10 Area Maritime Security Committees described earlier. We used those meetings to discuss, where applicable, the use of readers and costs and challenges of related Coast Guard rulemaking and delays. To analyze the results of these interviews, we synthesized the interview responses to identify common themes.

The perspectives we obtained during all interviews are not generalizable. However, they provide illustrative examples of, and important insights about, TWIC® program operations.

We conducted this performance audit from April 2024 to July 2026 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.

⁷RAND made recommendations for improving the Coast Guard's risk analysis determining those MTSA-regulated facilities that would be required to implement TWIC® readers. RAND's Homeland Security Operational Analysis Center, *Risk-Informed Analysis of Transportation Worker Identification Credential Reader Requirements* (Santa Monica, California.: 2022).

Appendix II: Transportation Security Administration's (TSA) Efforts to Streamline TWIC®

We recommended in 2007 and 2017 that the Department of Homeland Security (DHS) take steps to help streamline and harmonize its background check programs, including the Transportation Worker Identification Credential (TWIC®) and Hazardous Materials Endorsement (HME).¹ Specifically, in 2007 we recommended, among other things, that DHS describe in its coordination plan for conducting background investigations how it would establish and apply a common set of design and comparability standards to its credentialing programs. In 2017, we recommended that DHS explore with key critical infrastructure partners, whether and what opportunities existed to harmonize screening and credentialing access control efforts across critical infrastructure sectors. DHS implemented all 5 recommendations from these reports. TSA officials told us in May 2026 that the implementation of these recommendations by DHS and TSA helped shape the current structure and operations of TSA's transportation credentialing programs. Prior to 2007, these programs were largely organized into distinct and separate vetting programs, according to TSA officials. However, TSA officials said that since 2007 the agency has worked to consolidate the structure and processes across the transportation credentialing programs to help achieve the following efficiencies for these programs:

- Consolidating the Merchant Mariner and TWIC® enrollment by requiring Merchant Mariner applicants to first complete the required TWIC® enrollment, which TSA then provides to the Coast Guard for further vetting.²
- Coordinating with the Department of Defense to explore the feasibility of harmonizing the Common Access Card with the TWIC® card to allow TWIC® card holders to use their TWIC® card to access defense facilities. TSA was unsuccessful in implementing this harmonization due to the Department of Defense's different security and vetting standards for the Common Access Card, according to TSA officials.

In addition to these initiatives, TSA has streamlined some TWIC® operations, including by implementing online renewal for TWIC®,

¹GAO, *Transportation Security: DHS Efforts to Eliminate Redundant Background Check Investigations*, [GAO-07-756](#), (Washington D.C.: April 26, 2007). GAO, *Critical Infrastructure Protection: Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts*, [GAO-17-182](#), (Washington D.C.: Feb.7, 2017).

²Generally, subject to certain exceptions, mariners employed aboard U.S. merchant vessels greater than 100 gross register tons are required to have a valid U.S. Merchant Mariner Credential, which is issued by the Coast Guard. 46 U.S.C. § 8701; see 46 U.S.C. § 7302(a).

automating TSA PreCheck status, and reducing fees for TWIC® with other TSA credentialing programs.

Implementing online renewal. In 2022, TSA implemented an online renewal option for TWIC® holders. Applicants who choose to renew online can pay a reduced fee of \$116 compared to the in-person fee of \$124 for either a new or renewed card. According to TSA officials, online renewal saves applicants travel time and expenses because they do not have to physically travel to an enrollment center. Since TSA began tracking the measure, 86 percent of TWIC® card holders who chose to renew did so online.³

Automating TSA PreCheck® status. In 2020, TSA gave TWIC® and HME holders meeting certain eligibility requirements automatic TSA PreCheck® status without a separate application and at no additional cost.⁴ As of October 2024, approximately 2 million TWIC® holders and 250,000 HME holders have used their credentials to receive TSA PreCheck® status.

Reducing fees for workers with TWIC® and HME. Since TSA uses the same security threat assessment process for TWIC® and HME, the agency has implemented two specific fee-reduction measures for transportation workers who need both credentials: comparability and reciprocity. Comparability can provide a reduced fee process for some TWIC and all HME holders, while reciprocity eliminates entirely the need to pay a fee to TSA when using a TWIC to obtain an HME in participating states.

³Not all TWIC® holders are eligible to use online renewal. For example, non-U.S. citizens cannot renew their credential online due to the need to validate immigration-related documentation, such as visa expiration dates and validity.

⁴All active TWIC® and HME holders who are U.S. citizens, U.S. nationals, or lawful permanent residents and did not receive their TWIC® or HME via the waiver process can use their existing credentials to obtain TSA PreCheck® expedited screening.

**Fee Savings Associated with
Comparability**

The Transportation Security Administration maintains a public-facing website to share its fee structure by applicant type (e.g., first time applicant, renewing applicant doing so online, renewing applicant doing so in person). The standard Transportation Worker Identification Credential (TWIC®) applicant fee is \$124. If applicants already have a Hazardous Materials Endorsement (HME) and apply for a TWIC®, their fee will be \$93, resulting in a savings of \$31.

The standard HME enrollment fee is \$85.25. Depending on what state applicants live in, if they already have a TWIC® and apply for an HME, their fee will be \$41, resulting in a savings of \$44.25.

Source: GAO analysis of TSA documentation. |
GAO-26-107521

- **Comparability** allows for a potentially reduced application fee for those pursuing TWIC® and HME who use their existing security threat assessment when applying for the second credential.⁵ HME holders applying for a TWIC® can use comparability to acquire a TWIC® at a reduced fee regardless of what state they reside in because TSA, a federal agency, issues the credential. TWIC® holders applying for an HME can pursue a reduced fee HME by presenting their TWIC® only if they are residing in a participating state and after the state or territory confirms the presence of an existing and unexpired security threat assessment.⁶ In the 17 states that support full comparability, applicants have up to 4 years after receiving their TWIC® to use their existing security threat assessment for an HME. In the 10 states that support partial comparability, applicants must apply for the second credential in the first year after receiving their TWIC® to use their existing threat assessment.⁷
- **Reciprocity**, a measure that was required by statute in 2018, allows TWIC® holders to use their existing security threat assessment when applying for the HME credential without having to pay a fee to TSA.⁸ However, there is no reciprocity for HME holders who apply for TWIC®s due to the fact that the amended statute only concerns HME.⁹ Applicants in 11 states can use reciprocity as of fiscal year 2024 to obtain HMEs. Whether states choose to offer reciprocity is

⁵According to TSA officials, TSA does not reuse prior or existing security threat assessments when granting subsequent credentials. Rather, TSA takes official notice of the prior security threat assessment and previously granted credential in issuing the subsequent credential, according to officials.

⁶Some of the states that do not support comparability fall into a category that TSA refers to as "nonagent states." These eight states require applicants to use the state licensing agency instead of TSA's universal enrollment provider for HME. TSA officials stated that they could not speak to why states may impose this requirement, but they did share that the requirement entails an extra coordination step. Specifically, the state must first collect HME applicant information and then transmit it to TSA.

⁷Appendix III includes a map of U.S. states and territories with full, partial, or no comparability for HME for applicants with an existing TWIC®. Comparability for TWIC® holders applying for an HME is state dependent because the HME is issued by the state licensing agencies.

⁸See FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. K, tit. I, § 1978, 132 Stat. 3186, 3618 (codified at 49 U.S.C. § 5103a).

⁹See 49 U.S.C. § 5103a(a)(1)(B).

Example of a Non-Cost Effective Fee Reduction

James pays \$125.25 for a Transportation Worker Identification Credential (TWIC®) in January 2022, which is set to expire in January 2027 (given the 5-year lifespan of the security threat assessment on which issuance of the TWIC is based).

However, in January 2025, James identifies a career need for a Hazardous Material Endorsement (HME) on his existing Commercial Driver's License.

James lives in a state that offers full comparability, meaning James can take advantage of the reduced fee option that the Transportation Security Administration (TSA) offers, and use the security threat assessment on file from his TWIC® application to pursue the HME credential.

If James does this, the reduced application fee for the HME would be \$41. However, because the HME expiration date will tie to the expiration date of the security threat assessment on file, the \$41 expense buys James only two years of HME validity.

On the other hand, if James decides instead to undergo another security threat assessment and pay full price—\$85.25 (or \$44.25 more), James will gain three more years of holding the HME credential and secure the full five years of validity.

For James, the extra time (the full five years versus the abbreviated two years) may be more valuable than the cost savings.

The tradeoff: Applying for the HME credential using his previous security threat assessment satisfies James' immediate need for an HME, saves him some money up front, and eliminates the time and expense for another security threat assessment. However, it also costs James money later because the renewal for HME is on a shorter cycle, meaning that in 2027 James will have to reapply for both TWIC® and HME.

Source: GAO analysis of TSA documentation. | GAO-26-107521

- voluntary based on states' interests and capabilities.¹⁰ Per a TSA official, states can start or stop offering reciprocity at any time and can also do so whether or not they use TSA's enrollment provider. Minimally, states must be able to validate the TWIC® card's expiration date, check TSA's Canceled Card List, and notify TSA of the state's acceptance of the HME application.

According to TSA, some applicants may not opt to use the fee reduction options if they would not be cost effective or if the applicants live in states that cannot support comparability. The fee reduction options may not be cost effective for some applicants because approval of a credential using a reduced fee option only grants credential validity for the remaining time left on the 5-year security threat assessment on which the issuance of the credential is based. See the sidebar for a hypothetical example in which the fee reduction option would not be cost effective.

To assist with the implementation of comparability and reciprocity, TSA has also provided training and guidance to drivers' licensing agencies in states that issue the HME credential based on an existing TWIC® on how to ensure that the expiration dates of the credentials will align. In addition, TSA officials stated that the agency is updating its online portal to provide more detailed information on TWIC® security threat assessments and to improve functionality. Specifically:

- In fiscal year 2025, TSA plans to add information specific to TWIC® security threat assessment statuses and expiration dates to the general information it already communicates about HME security threat assessment statuses, according to TSA officials. TSA officials stated that this additional information will ease states' abilities to validate the TWIC® when issuing an HME.
- As of December 2025, TSA officials told us that they were working to update and improve the portal's functionality in response to concerns some state officials expressed about the portal technology being outdated and incompatible with their systems.

TSA officials told us that coordinating with some states and territories on TWIC® and HME can be challenging. States and territories have a significant role in HME program administration and TSA cannot compel states' participation in credentialing reform efforts. According to TSA, some states do not have the necessary technology to interface with

¹⁰According to TSA officials, the 11 states where applicants used their TWIC® security threat assessment to receive an HME are: Alabama, California, Hawaii, Idaho, Illinois, Iowa, Maryland, Utah, Virginia, Washington, and Wyoming.

TSA's systems that would share expiration dates for the credentials and do not have a large enough demand to upgrade this technology.

Factors Affecting Streamlining Efforts

In December 2024, during the course of our audit, Congress passed the Transportation Security Screening Modernization Act of 2024.¹¹ The act requires TSA to take necessary actions within two years to streamline the procedures for individuals applying for or renewing enrollment in more than one TSA security threat assessment program, in particular, in TWIC® and HME.¹² Among other things, this streamlining must permit applicants to enroll at any TSA enrollment center once for a threat assessment program endorsement and use the application to enroll in other programs.¹³ TSA plans to make the following additional improvements to streamline enrollment for the TWIC® and HME credentials, in response to the Act's requirements:

- Implement online enrollment and renewals for eligible HME holders by adding a facial photo capture into the HME enrollment process, allowing eligible HME holders to complete their application entirely online.
- Provide states with improved access to security threat assessment data to support HME issuance based on a cardholder's existing TWIC® card
- Develop a consolidated process that will enroll applicants in the TWIC® and HME programs at once
- Regularly review and adjust security threat assessment fees to ensure the minimum cost for enrollment necessary to cover services like vetting, data collection, case management, and card printing and issuance.

TSA officials told us in May 2026 that they are planning to develop a unified enrollment workflow to further standardize enrollment for the TWIC® and HME credentials, add facial photo capture into the HME enrollment process, and update the state portal to improve state licensing agencies' access to security threat assessment data by December 23 2026, the deadline specified by the Transportation Security Screening Modernization Act of 2024. Additionally, TSA officials said that they held a webinar for states in April 2026 to provide information on reciprocity and

¹¹ Pub. L. No. 118-202, 138 Stat. 2688.

¹² Pub. L. No. 118-202, § 3, 138 Stat. at 2688-89.

¹³ Pub. L. No. 118-202, § 3(a)(1)(A), 138 Stat. at 2688-89.

navigating the state portal to access security threat assessment data as well as working with states to correct state-submitted HME records in the state portal.

TSA also reported limitations in further streamlining TWIC® and HME. TSA officials attributed these limitations in part to challenges the agency faces in coordinating with some states and territories on TWIC® and HME and to the National Crime Prevention and Privacy Compact Act of 1998 (Compact Act).¹⁴

State and territory coordination. States and territories have a significant role in HME program administration and TSA cannot compel states' participation in credentialing reform efforts. According to TSA, some states do not have the necessary technology to interface with TSA's systems that would share expiration dates for the credentials and do not have a large enough demand to upgrade this technology.

Compact Act: This act provides the legal framework for the establishment of a cooperative federal-state system for the interstate exchange of criminal history records for noncriminal justice uses when authorized by federal or state law.¹⁵ It governs the process by which states and federal agencies, including TSA, obtain criminal history records through the FBI for authorized non-criminal justice purposes including conducting security threat assessments for TWIC®.¹⁶ The

¹⁴The act authorizes signatory states, as well as the FBI as the national repository, to make available all unsealed criminal history records from their repositories in response to authorized fingerprint-based noncriminal justice background checks, including from TSA. National Crime Prevention and Privacy Compact Act of 1998, Pub. L. No. 105-251, tit. II, subtit. A, §§ 211-217, 112 Stat. 1870, 1874-84 (codified as amended at 34 U.S.C. §§ 40311-40316). TSA submits such background check requests when conducting TWIC® and HME security threat assessments, since these criminal history records are part of the applicants' overall security threat assessment packages.

¹⁵As of July 2025, the 37 states which are signatories under the Compact Act are AK, AZ, AR, CO, CT, DE, FL, GA, HI, ID, IA, KS, LA, NE, ME, MD, MI, MN, MS, MO, MT, NV, NH, NJ, NY, NC, OH, OK, OR, SC, TN, UT, VT, VA, WA, WV, WY. Additionally, 9 states and territories have signed a memorandum of understanding to voluntarily abide by the Compact and the Council's rules, procedures, and policies regarding the noncriminal justice use of the Interstate Identification Index without ratifying the Compact: IL, KY, MA, NM, ND, SD, AS, GM, and PR. As of July 2025, the 10 non-signatory states, district, and territories are AL, CA, MP, DC, IN, PA, RI, TX, WI, and VI.

¹⁶The Compact Act also established the Compact Council, a council appointed by the U.S. Attorney General that has authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) for noncriminal justice purposes. 34 U.S.C. § 40316, art. VI, (a), (b), (e).

Compact Act allows for TSA to submit applicant fingerprints to FBI and receive criminal history records for those applicants. The Compact Act requires that the Compact Council establish standards to ensure that records obtained under the Compact Act are used only for authorized purposes and “require that subsequent record checks are requested to obtain current information whenever a new need arises.”¹⁷ While the Compact Act does not address the reuse of fingerprints in requesting criminal history records, it does require requesting agencies to submit subject fingerprints or other approved forms of positive identification with all requests for criminal history record checks for noncriminal justice purposes.¹⁸ In 2010, the FBI approved a policy that allowed for the reuse of applicant fingerprints for the same purpose as the original fingerprint submission. The Compact Council reevaluated the FBI’s 2010 policy on the reuse of fingerprints and subsequently established a new policy governing the reuse of fingerprints for different noncriminal justice purposes in May 2024.

In October 2024, TSA officials stated that they wanted to further streamline processes for applicants who possess either a TWIC® or an HME to obtain the other credential by reusing applicant fingerprints when conducting a second security threat assessment. TSA officials stated that this would allow applicants to apply for a second credential without having to travel to an enrollment center for a second time to be fingerprinted again. However, in order to follow the FBI’s policy on reusing fingerprints that required agencies to obtain a new set of fingerprints for each separate noncriminal justice purpose, TSA officials said that they had to require that some applicants visit enrollment centers to submit a second set of fingerprints.¹⁹ Accordingly, TSA officials told us in October 2024 that the FBI’s policy on the reuse of applicant fingerprints prevented TSA

¹⁷34 U.S.C. § 40316, art. IV(c).

¹⁸See 34 U.S.C. § 40316, art. V, (a).

¹⁹While comparability allows some individuals applying for multiple credentials to avoid re-fingerprinting, others would need to return to be fingerprinted again. For example, TSA officials told GAO that some applicants who already have a TWIC® or HME may choose to not pursue a fee reduction when applying for a second credential for several reasons, including a desire to have both credentials for a full five years; these applicants would need to return for re-fingerprinting under the prior FBI’s policy on reusing fingerprints. Under the new Compact Act policy, if TSA were to put measures in place to implement this policy, such individuals would not need to return for re-fingerprinting as long as all requirements were met, according to TSA and Federal Bureau of Investigation officials.

from streamlining the process by using the same set of applicant fingerprints for multiple credentials.

During the course of our audit, in May 2025, the FBI's policy to allow the reuse of fingerprints for noncriminal justice purposes was published, including the policy language and technical requirements for implementation. One such requirement is that agencies conduct a biometric identity verification for each individual prior to reusing their fingerprints. The FBI disseminated guidance on the policy to federal and state agencies in June 2025. As a result of the policy change, FBI officials said that TSA may reuse applicant fingerprints for multiple security threat assessments when consistent with the FBI's policy.²⁰ FBI officials stated that the biometric identity verification requirement exists to confirm the identity of applicants as the same individuals who submitted the initial fingerprints.

According to FBI officials, agencies are responsible for determining the method of biometric identity verification to be used under the new policy, which may then be approved by designated federal officials. According to agency officials, the Compact Council discussed which forms of biometric verification would be acceptable under this policy but intentionally did not define biometric identity verification within the policy to provide agencies flexibility during implementation. These officials said that since the use of this policy requires approval by the appropriate federal official, TSA would need to coordinate with its respective Criminal Justice Information Services Systems Officer or designated federal official to determine the method that would best meet the agency's needs while also meeting the requirements of the policy. While the Compact Council did not state which kinds of biometric identity verification would be acceptable under the new policy, generally, agencies could consider implementing a remote identity verification method that may meet the policy's criteria. However, TSA officials said they do not have an existing method to remotely verify identities and as of December 2025, did not have plans to explore the feasibility of remote identity verification.

²⁰According to the FBI's updated policy, when approved by an appropriate state or federal official, an agency or entity may be authorized to reuse applicant fingerprints for submission to the FBI when each of the following criteria are met: the agency or entity is authorized by law to conduct the national fingerprint-based background check and retain the fingerprints; the applicant is initiating the request for which the agency or entity is authorized to submit fingerprints; a biometric identity verification is conducted prior to reuse of the fingerprints; the applicant fingerprints were not previously rejected by the FBI for image quality standards.

TSA officials said that a significant portion of the applicants who need both the HME and TWIC® credentials can use comparability and reciprocity, depending on which credential they hold, to avoid a second security threat assessment. Officials estimated that the number of applicants who need both credentials and live in a state that does not allow for comparability as a small percentage in comparison to the percentage of applicants who could use comparability. From fiscal years 2019 through 2024, the percentage of TWIC® applicants who used a reduced fee enrollment was less than 1 percent annually, and the percentage of HME applicants who used a reduced fee enrollment was less than 3 percent annually, according to TSA data. TSA officials attributed these percentages to the low number of truck drivers—a primary consumer of the reduced fee enrollment—who hold an HME and are also in need of a TWIC® card. According to TSA officials, the Federal Motor Carrier Safety Administration estimated that 11 percent of U.S. truck drivers have an HME, thus limiting the pool of eligible reduced fee enrollment applicants. One of the stakeholders we contacted who represents commercial motor vehicle safety officials and industry representatives estimated that approximately 5 to 10 percent of their members need both the TWIC and HME credentials. Similarly, an additional stakeholder representing members of the tank trucking industry said that the majority of its membership require an HME but that only about 10 to 15 percent of its membership also hold a TWIC® card.

Furthermore, officials said that due to the need to develop new internal procedures, potentially promulgate a new rule, and revise applicant fees, they were not considering exploring and implementing a method for identity verification that would satisfy the requirements outlined in the new policy. TSA officials stated that they viewed continuing to rely on comparability and reciprocity as a more cost-beneficial approach but were taking steps, such as developing plans to collect applicant photos, that could potentially enable remote verification in the future.

In February 2026, the President issued an executive order stating that the “Attorney General shall provide DHS with access, for purposes related to DHS’s screening and vetting missions and to maximum extent permitted by law, to criminal history information records available to or maintained by the Department of Justice.”²¹ According to TSA officials in May 2026, TSA and FBI’s Criminal Justice Information Services division are

²¹*Protecting the National Security and Welfare of the United States and Its Citizens from Criminal Actors and Other Public Safety Threats*, Exec. Order 14,385, § 2, 91 Fed. Reg. 6,505 Feb. 6, 2026.

continuing to discuss implementation of the executive order. TSA officials stated that they have been advised to use an “intelligence” purpose code when requesting information from FBI for security threat assessments, but that they have yet to ascertain from FBI whether records obtained under that purpose code may be used for multiple credentialing programs.

Review of TWIC® and HME Fees

Regarding regular reviews of TWIC® and HME fees, TSA is to review the TWIC® and HME fees biennially to fully recover costs related to the programs over a five-year period. In its fiscal year 2024 review of the TWIC® fee, TSA estimated that the TWIC® program cost TSA a total of \$315 million over this five-year period. TSA then divided these total costs by the 2,659,000 total estimated interactions with the TWIC® program over five years, including new or renewing in person enrollments, online renewals, new or renewing reduced fee enrollments, and lost or damaged card replacements.

To project total costs for the TWIC® program, TSA determined the average amount of collections, obligations and expenses, and unobligated carryover balances for the 5 prior fiscal years— 2019 through 2023. TSA projected the total annual costs of the TWIC® program for fiscal years 2024 and 2025 as \$70 million with a projected revenue for fiscal year 2024 of \$72 million and \$67 million for fiscal year 2025.

To determine cost recovery over the prior 5 fiscal years, TSA compares the total amount of fees collected and eligible expenses to identify a percentage of costs recovered through fee collection. TSA determined that they recovered an average of 99 percent of TSA's TWIC® program costs through fee collection over this period. TSA reviews the HME fee using a similar process but instead of dividing the total HME program costs by estimated interactions with the program, TSA uses the number of estimated HME applicants over the 5 prior fiscal years to help determine total costs and cost recovery, as shown in table 2.

Appendix II: Transportation Security
Administration's (TSA) Efforts to Streamline
TWIC®

Table 2: Summary of TWIC® and HME Fee-setting for Fiscal Years 2024 and 2025

Credentialing program	Average collections for fiscal years 2019-2023	Average obligations and expenses for fiscal year 2019-2023	Projected costs for fiscal years 2024 and 2025	Projected revenue for fiscal years 2024 and 2025	Average cost recovery percentage for fiscal years 2019-2023
TWIC®	\$62 million	\$63 million	\$70 million (both fiscal years)	\$72 million (fiscal year 2024) \$67 million (fiscal year 2025)	99 percent
HME	\$18 million	\$17 million	\$18 million (both fiscal years)	\$19 million (fiscal year 2024) \$18 million (fiscal year 2025)	102 percent

Source: GAO analysis of TSA fee-setting documentation. | GAO-26-107521

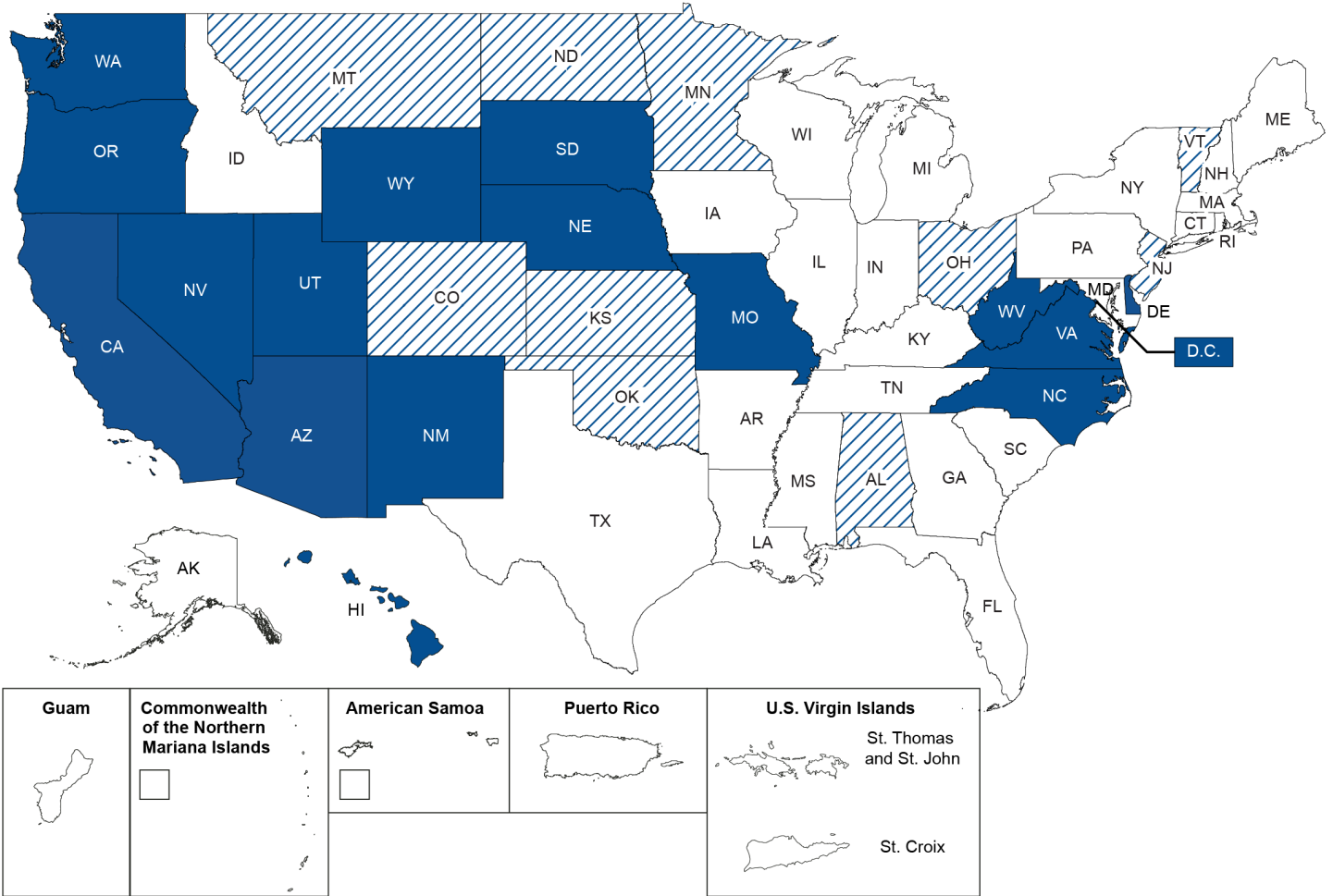
Appendix III: States and Territories with Comparability for the Hazardous Materials Endorsement (HME)

The Transportation Security Administration (TSA) has the same security threat assessment requirements for both the Transportation Worker Identification Credential (TWIC®) and HME, which allows TSA to implement a concept known as comparability across the programs. Applicants who could use comparability and are already holding a TWIC® would not have to undergo a second security threat assessment when pursuing an HME—and vice versa. Not all states have the information technology systems capable of integrating TSA’s security threat assessment into their processes for administering the HME. This is because an HME is tied to an applicant’s commercial driver’s license, which states issue through their licensing agencies, rather than a standalone credential. As a result, the state must be able to issue the HME with an expiration date that aligns with the expiration date of the commercial driver’s license. To use an applicant’s existing security threat assessment to issue an HME, states must have the systems in place to verify the validity of the assessment and the TWIC® credential. Because states have variations in their overall system capabilities and varying commercial driver’s license expiration dates, some states can support full comparability, some can support it partially, and some cannot support it at all.

Figure 12 outlines the U.S. states and territories that have full, partial, or no comparability for the HME credential for applicants with an existing TWIC®.

Appendix III: States and Territories with Comparability for the Hazardous Materials Endorsement (HME)

Figure 12: U.S. States and Territories with Comparability for Hazardous Materials Endorsement (HME) for Applicants with an Existing Transportation Worker Identification Credential (TWIC®)



Legend

- Full comparability:** States that can issue an HME to an individual if the applicant has an existing, valid TWIC® Security Threat Assessment with at least one year remaining before expiration.^a
- Partial comparability:** States that have the capability to issue an HME based on an existing, valid TWIC® Security Threat Assessment with at least four years remaining before expiration.^b
- States and territories that do not offer the option to use an existing TWIC® for an HME applicant

Source: GAO analysis of TSA comparability data; U.S. Census Bureau (map). | GAO-26-107521

^aIn states that offer full comparability, applicants have up to 4 years after receiving their TWIC® to use their existing security threat assessment for an HME.

^bIn states that offer partial comparability, applicants must apply for the second credential in the first year after receiving their TWIC® to use their existing security threat assessment.

**Appendix III: States and Territories with
Comparability for the Hazardous Materials
Endorsement (HME)**

States that offer full comparability: AZ, CA, DE, DC, HI, MO, NC, NE, NM, NV, OR, SD, UT, VA, WA, WV, WY.

States that offer partial comparability: AL, CO, KS, MN, MT, ND, NJ, OH, OK, VT.

States and territories that do not offer comparability: AK, AR, CT, FL, GA, ID, IL, IN, KY, IA, LA, MD, ME, MA, MI, MS, NH, NY, RI, SC, TN, WI, American Samoa, Guam, Commonwealth of the Northern Marianas, Puerto Rico, and the U.S. Virgin Islands.

Appendix IV: Performance Measurement System for the Transportation Worker Identification Credential (TWIC®)

The Transportation Security Administration (TSA) has developed a performance measurement system to monitor TWIC® operations to comply with Department of Homeland Security (DHS) and Office of Management and Budget reporting requirements, according to TSA officials.¹ This system includes performance measures for the overall program and performance measures for TSA’s contracted enrollment centers. TSA has several activities in place to monitor enrollment centers’ performance, and to measure customer satisfaction

Performance measures for the overall program. TSA has nine measures that it uses to monitor overall program performance. TSA officials told us that the agency reports on its operational performance measures on the Office of Management and Budget’s publicly available website. See table 3 for examples from the nine measures.

Table 3: Examples of Performance Measures for the Transportation Worker Identification Credential (TWIC®) Program

Performance measure	Purpose
Average adjudication total accuracy rate	Tracks the overall accuracy with which TSA conducts security threat assessments. This measure evaluates whether TSA correctly conducted manual reviews for applicants and accounts for any administrative errors in the review.
Invalid enrollment rate	Tracks the number of applicants that TSA incorrectly enrolled for a TWIC®. Errors can include data entry errors by an applicant or enrollment agent, the applicant providing unacceptable or mismatched identification documents, or an invalid record of the applicant’s identification documents.
Average wait time	Tracks the average wait time that an applicant waits to begin enrollment or card activation, measured from the time the applicant arrives at the enrollment center to when enrollment or card activation begins.
Operational availability	Tracks the percentage of time that TWIC® enrollment centers are open and processing enrollments and card activations against the total scheduled hours of operation for the network of enrollment centers.
Online renewals	Tracks the percentage each month of individuals renewing their TWIC® online against the total number of renewals that would be eligible for TWIC® online renewal.

Source: GAO summary of Transportation Security Administration information. | GAO-26-107521

TSA officials said they review each of the nine measures routinely and refine them as needed, sometimes adding or removing measures based

¹According to TSA, the nine performance measures for TWIC® represent the operational metrics the Office of Management and Budget requires in its Circular A-11 Section 55. Officials said that the requirement for developing and monitoring performance measures is found in Circular No. A-11 Part 7 and mandated by 40 U.S.C. § 11302. TSA reports its operational performance measures publicly on the Office of Management and Budget’s IT Dashboard.

on DHS and Office of Management and Budget requirements. For example, TSA most recently added the measure to track the percentage of TWIC® renewals done through the online renewal feature. According to TSA officials, the agency has generally met its performance goals for the TWIC® program.

Performance measures for TSA’s contracted enrollment centers.

TSA has 25 performance measures to monitor its approximately 530 enrollment centers and contractor operations and has formal acceptable quality levels, or minimum required levels of performance, for some of these measures.² For example, TSA’s contracted enrollment provider measures system availability, or the percentage of time that their services, such as in-person enrollment and website functionality, are correctly working. According to TSA documentation, the minimum required level of this measure is 99 percent.

Furthermore, TSA assesses data on measures without formal acceptable quality levels, such as the number of enrollment centers with chronic wait time issues.³ When performance does not meet the acceptable level, or shows cause for concern if no level exists, TSA officials generally delegate resolution of individual center issues to their provider. Similarly, TSA can also request a formal corrective action plan for broad and significant issues. Officials said that the development of a plan is rare, and they could not recall the last time they had to request one from the provider.

TSA officials said that in addition to monitoring the performance of enrollment centers, they also regularly meet with the contracted enrollment center provider to discuss, among other topics, the expansion of enrollment center locations based on market demand. The contracted enrollment center provider has proposed establishing additional enrollment centers which while not required by the contract, is highly

²TSA officials said that they evaluate which measures need or no longer need formal acceptable quality levels with each contract iteration for their enrollment provider. When determining if a measure needs an acceptable quality level, TSA considers factors such as the existence of a performance difference that impacts the customer experience and historical issues for the enrollment centers. Officials said that some measures may no longer need a formal acceptable quality level if the data has reached a satisfactory level of stability, though they still collect data on those measures.

³TSA documentation defines enrollment centers with chronic wait time issues as enrollment centers that exceed the acceptable quality level for average wait times for both appointments or walk-ins—5 minutes and 15 minutes, respectively—for 3 weeks out of a 4-week reporting period.

encouraged by TSA, according to TSA officials. Regarding access to enrollment centers in rural areas, none of the officials from 10 Area Maritime Security Committees we interviewed raised the issue of a lack of access to enrollment centers in rural areas. Officials from 1 of the 10 Committees stated that their port's access to enrollment centers has significantly improved with the establishment of additional centers. One of the industry stakeholders we contacted who represents the trucking industry told us they have raised the issue of a lack of enrollment centers, particularly in rural areas, with TSA. Specifically, these same officials said that there is a critical lack of enrollment centers in rural areas, particularly in Alaska, Idaho, and the Midwest.

We found through our analysis of the number of fiscal year 2024 TWIC® enrollments by enrollment center that 38 percent of the total 607 enrollment centers that processed a TWIC® enrollment were located in rural areas, as defined by the U.S. Census Bureau.⁴ Rural enrollment centers accounted for approximately 33 percent of all TWIC® enrollments for fiscal year 2024. Table 4 shows the percentage of TWIC® enrollments processed by rural enrollment centers in selected states.

⁴The U.S. Census Bureau defines rural areas as all geographic areas that are not classified as urban. The Census Bureau defines "urban areas" as either urbanized areas, which contain 50,000 or more people or urban clusters, which have at least 2,500 people but fewer than 50,000 residents.

Appendix IV: Performance Measurement
System for the Transportation Worker
Identification Credential (TWIC®)

Table 4: Percentage of TWIC® Enrollments Processed by Rural TSA Enrollment Centers in Selected States

State	Total number of TSA enrollment centers	Total number of rural TSA enrollment centers	Percentage of total TWIC® enrollments by state processed by rural TSA enrollment centers
Alaska	14	6	15 percent
Idaho	4	1	16 percent
Midwest region ^a			
Illinois	23	13	74 percent
Indiana	17	7	45 percent
Iowa	5	1	37 percent
Kansas	9	3	16 percent
Michigan	19	6	46 percent
Minnesota	6	3	79 percent
Missouri	10	4	45 percent
Nebraska	6	0	0 percent
North Dakota	3	0	0 percent
Ohio	22	7	19 percent
South Dakota	2	0	0 percent
Wisconsin	7	2	35 percent

Source: GAO analysis of TSA enrollment center and U.S. Census Bureau data. | GAO26-107521

^aThe U.S. Census Bureau defines the Midwest region as: Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin.

Monitoring activities for contracted enrollment centers. TSA officials engage in several monitoring activities to assess the performance of their contracted enrollment centers: regular status reports, in-person site visits, and quality control assessments.

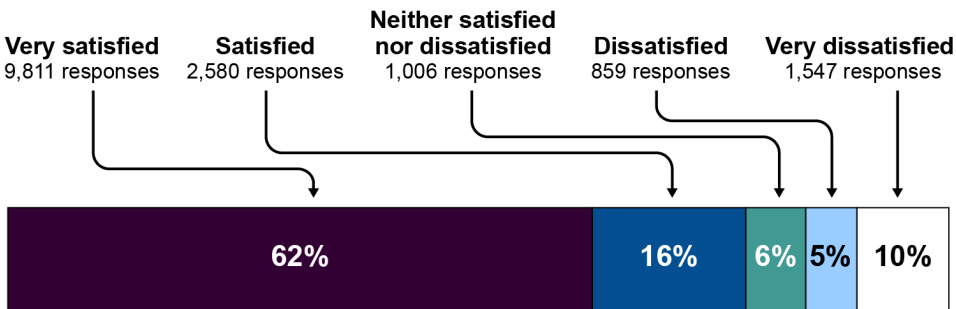
- **Status reports.** TSA monitors the contractor's performance frequently by requiring weekly and monthly status reports for enrollment centers. Weekly reports can include topics such as enrollment center relocations or openings while monthly reports can include topics such as call center call volumes.
- **Site visits.** To observe the contractor's performance and interactions with applicants, TSA conducts site visits to enrollment centers. During the visits, officials use a checklist that addresses various aspects of center operations, such as the appearance of the center and enrollment workflow. TSA officials told us that they use applicant wait times, enrollment volumes, when the center was last visited, and stakeholder complaints to prioritize centers for Transportation Surface

Inspectors to visit. They said each month, TSA reviews the findings from the recent visits and escalates any deficiencies to the provider requiring attention. They then document the provider's corrections.

- **Quality control assessments.** The contractor is responsible for these, in part to supplement TSA's own evaluations. During these assessments, contractor staff photograph various aspects of the enrollment center. If staff document any deficiencies or issues, such as outdated signage, malfunctioning technology, or staff not greeting applicants in a timely fashion, the center has five business days to correct it.

Customer satisfaction surveys. TSA's contractor disseminates a survey to any visitor of its enrollment centers and provides online access to it. The survey asks applicants to rate their level of satisfaction with their overall in-person enrollment services experience and with the resolution if they had an issue with the in-person enrollment experience. For example, the most recent available data from fiscal year 2025 (as of July 2025) show that approximately 80 percent of the 5,787 respondents said that they were either satisfied or very satisfied with the services they received at the enrollment center with a response rate of about 3%, as shown in figure 13. While TSA did not report having a target for customer satisfaction, officials told us that they generally monitor applicant feedback data.

Figure 13: Enrollment Center Visit Survey Results for Transportation Worker Identification Credential (TWIC®) Applicants from Fiscal Year 2023 to July 2025



Source: GAO analysis of TSA survey data. | GAO-26-107521

Appendix V: Timeline for Transportation Worker Identification Credential (TWIC®) Reader Implementation

Table 5 describes Coast Guard’s proposed and final rules, laws, and GAO recommendations for implementing the TWIC® readers.

Table 5: Transportation Worker Identification Credential (TWIC®) Card Reader Timeline for Regulated Facilities

Date	TWIC® reader-related event	Source
October 2006	The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) required the Secretary of Homeland Security (DHS) ^a to conduct a TWIC® reader pilot program and promulgate within 2 years of commencing this program the final regulations requiring the deployment of TWIC® readers.	Pub. L. No. 109-347, § 104, 120 Stat. 1884, 1889-90 (2006).
March 2009	The Coast Guard published an advanced notice of proposed rulemaking discussing preliminary thoughts on how it could determine the risk level and associated TWIC® reader requirements for three categories of facilities—Risk Groups A, B, and C ^b —in order of descending risk level. This proposed rule would only require facilities within Risk Group A—including those that carry and handle Certain Dangerous Cargoes ^c in bulk—and Risk Group B—including those that carry and receive vessels that carry hazardous materials that are not Certain Dangerous Cargoes in bulk—to implement TWIC® readers. Facilities in Risk Group C would only be required to visually inspect TWIC® cards.	Transportation Worker Identification Credential (TWIC)—Reader Requirements, 74 Fed. Reg. 13,360 (Mar. 27, 2009).
May 2011	GAO recommended that DHS conduct an effectiveness assessment that evaluated whether the use of TWIC® in its present form (2011) and planned use with readers would enhance the posture of security beyond efforts already in place, given costs and program risks.	GAO-11-657 , Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives
March 2013	The Coast Guard published a notice of proposed rulemaking, in which the main change in approach from the advanced notice of proposed rulemaking would be to require only Risk Group A facilities to electronically read TWIC® cards. Risk Group B and C facilities would continue visually inspecting TWIC® cards.	Transportation Worker Identification Credential (TWIC)—Reader Requirements, 78 Fed. Reg. 17,782 (Mar. 22, 2013).
May 2013	GAO reported that the TWIC® card reader pilot results were unreliable and that the program’s benefits needed to be reassessed. We recommended that Congress consider repealing the requirement that DHS promulgate final regulations requiring the implementation of card readers that are consistent with the findings of the pilot program. Instead, we recommended that Congress consider requiring DHS to first complete an assessment that evaluated the effectiveness of using TWIC® with readers for enhancing port security, as recommended in our May 2011 report, and then use the results of this assessment to promulgate a final regulation as appropriate.	GAO-13-198 , Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed

**Appendix V: Timeline for Transportation
Worker Identification Credential (TWIC®)
Reader Implementation**

Date	TWIC® reader-related event	Source
January 2014	In response to GAO's May 2013 report, the explanatory statement accompanying the Consolidated Appropriations Act, 2014, directed DHS to complete the recommended assessment by April 17, 2014.	160 Cong. Rec. H475, H927 (daily ed. Jan. 15, 2014) (accompanying Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, 128 Stat. 5).
August 2016	The Coast Guard published a final rule, effective August 23, 2018, which, among other changes from the notice of proposed rulemaking, eliminated the distinction between Risk Groups B and C. The final rule also eliminated the special requirement that barge fleeting facilities that handle or receive barges carrying Certain Dangerous Cargoes in bulk be classified as Risk Group A.	Transportation Worker Identification Credential (TWIC)—Reader Requirements, 81 Fed. Reg. 57,652 (Aug. 23, 2016).
December 2016	The Transportation Security Card Program Assessment Act was enacted, which, among other things, required DHS to commission an assessment of the effectiveness of the TWIC® program at enhancing security and reducing security risks for regulated facilities and vessels. (We reviewed this assessment and used its recommendations to inform this work.)	Pub. L. No. 114-278, § 1(b), 130 Stat. 1410 (2016).
June 2018	In response to a 2017 petition requesting revisions to the 2016 reader rule, the Coast Guard published a second notice of proposed rulemaking, which proposed delaying implementation of the 2016 TWIC® reader rule until August 23, 2021 for Risk Group A facilities that: 1. handle Certain Dangerous Cargoes in bulk, but do not transfer these cargoes to or from a vessel, and 2. receive vessels carrying Certain Dangerous Cargoes in bulk, but do not, during that vessel-to-facility interface, transfer these bulk cargoes to or from those vessels.	TWIC-Reader Requirements; Delay of Effective Date, 83 Fed. Reg. 29,067 (June 22, 2018).
August 2018	The Transportation Worker Identification Credential Accountability Act of 2018 was enacted, prohibiting DHS from: (1) implementing the 2016 TWIC® reader rule; and (2) revising such rule—except to extend its effective date—or any other rule requiring readers for biometric transportation security cards under 46 U.S.C. § 70105(k)(3), until at least 60 days after the results of the Transportation Security Card Program Assessment are submitted to Congress as required in the December 2016 act.	Pub. L. No. 115-230, § 2, 132 Stat. 1631.

**Appendix V: Timeline for Transportation
Worker Identification Credential (TWIC®)
Reader Implementation**

Date	TWIC® reader-related event	Source
March 2020	The Coast Guard published a final rule which extended the effective date of the 2016 TWIC® reader rule until May 8, 2023 for facilities that: 1. handle Certain Dangerous Cargoes in bulk, but do not transfer them to or from a vessel; 2. handle Certain Dangerous Cargoes in bulk, and do transfer them to or from a vessel; and 3. receive vessels carrying Certain Dangerous Cargoes in bulk, but do not, during that vessel-to-facility interface, transfer these bulk cargoes to or from those vessels. The final rule extended the effective date of the 2016 TWIC® reader rule until June 8, 2020 for facilities that receive vessels certificated to carry more than 1,000 passengers. However, the Coast Guard reported that it delayed implementation until 2020 and enforcement of this regulation until January 1, 2022, due to the COVID-19 pandemic.	TWIC-Reader Requirements; Delay of Effective Date, 85 Fed. Reg. 13,493 (Mar. 9, 2020).
July 2022	The Coast Guard received its 2020 commissioned report from RAND that estimated that between 471 to 711 facilities would likely be subject to the reader delay.	RAND, Homeland Security Operational Analysis Center, Risk-Informed Analysis of Transportation Worker Identification Credential Reader Requirements
December 2022	To allow time for the Coast Guard to evaluate RAND's analysis, the Coast Guard proposed delaying the effective date of the TWIC® reader rule for facilities that handle, and receive vessels carrying, Certain Dangerous Cargoes in bulk to May 8, 2026. Following this proposed delay, the 2023 National Defense Authorization Act adopted May 8, 2026 as the statutorily required earliest date of implementation of TWIC® readers for all facilities that were subject to the March 2020 delay rule (covered facilities).	Transportation Worker Identification Credential (TWIC)-Reader Requirements; Second Delay of Effective Date, 87 Fed. Reg. 74,563 (Dec. 6, 2022). James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, div. K, tit. CXVIII, § 11804(c), (d), 136 Stat. 2395, 4164.
April 2023	In response to the December 2022 statutory amendment, the Coast Guard published a Conforming Amendment in regulation which changed the implementation date to May 8, 2026 for covered facilities.	Transportation Worker Identification Credential-Facility Reader Requirement; Conforming Amendment, 88 Fed. Reg. 23,349 (Apr. 17, 2023).
October 2024	The Coast Guard delayed the effective date for TWIC® reader implementation for covered facilities until May 8, 2029.	TWIC-Reader Requirements; Second Delay of Effective Date, 89 Fed. Reg. 86,723 (Oct. 31, 2024).

Source: GAO summary of Transportation Security Administration information, Coast Guard information, statutes, regulations, and GAO reports. | GAO-26-107521

Notes: For the purposes of this appendix, "MTSA-regulated facilities" refer to those regulated in 33 C.F.R. pt. 105. See 33 C.F.R. § 105.105(a). While the timeline concerns regulated facilities, many of the actions discussed also affected vessels and Outer Continental Shelf (OCS) facilities regulated in 33 C.F.R. pts. 104 and 106.

^aThe Security and Accountability for Every Port Act of 2006 (SAFE Port Act) amended 46 U.S.C. § 70105 to require the Secretary of the department in which the Coast Guard is operating to conduct a card reader pilot program and promulgate final regulations requiring the deployment of card readers consistent with the finding of the pilot program. Pub. L. No. 109-347, § 104, 120 Stat. 1884, 1889-90. For the purposes of this Appendix, "DHS" refers to the Secretary of the department in which the Coast Guard is operating, as DHS has been the department in which the Coast Guard was operating during the course of this review.

**Appendix V: Timeline for Transportation
Worker Identification Credential (TWIC®)
Reader Implementation**

^bUnder the advance notice of proposed rulemaking, the Risks Groups would be for vessels and facilities regulated under 33 C.F.R. parts 104 and 105. All OCS facilities regulated under 33 C.F.R. part 106 would fall into Risk Group B. For facilities, Risk Group A would consist of (1) facilities that handle Certain Dangerous Cargoes in bulk; (2) facilities that receive vessels certificated to carry more than 1,000 passengers; and (3) barge fleet facilities that receive barges carrying Certain Dangerous Cargoes in bulk. For a full list of proposed Risk Groups B and C, which were eventually eliminated, see 74 Fed. Reg. 13,360 (Mar. 27, 2009).

^cCertain Dangerous Cargoes include certain forms of fuming sulfuric acid and chlorine. 33 C.F.R. §§ 101.105, 160.202.

Appendix VI: Comments from the Department of Homeland Security

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



**Homeland
Security**

BY ELECTRONIC SUBMISSION

April 22, 2026

Tina Won Sherman
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-107521, "TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL: Actions Needed to Address Maritime Security Risks"

Dear Ms. Sherman,

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (hereafter referred to as "the auditors") work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note the auditors' acknowledgment that the Transportation Security Administration (TSA) took steps to communicate Transportation Worker Identification Credential program information with stakeholders, and that the U.S. Coast Guard took action to address stakeholder concerns by conducting a risk analysis for which types of facilities it will require to implement Transportation Worker Identification Credential readers. DHS remains committed to delivering communication enhancements to stakeholders, along with strengthening planning and data sharing and conducting quality inspections. Protecting the security of access to designated secure areas for vessels and facilities is a critical step to ensuring the safety of the maritime transportation system.

The draft report contained seven recommendations with which the Department concurs. Enclosed find our detailed responses to each recommendation. DHS previously submitted technical comments addressing accuracy, contextual, and other issues under a separate cover for the auditors' consideration, as appropriate.

**Appendix VI: Comments from the Department
of Homeland Security**

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.

Sincerely,

JEFFREY M. BOBICH  Digitally signed by
JEFFREY M. BOBICH
Date: 2026.04.22
17:55:01 -04'00'

JEFFREY M. BOBICH
Director of Financial Management

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-26-107521**

GAO recommended the TSA Administrator:

Recommendation 1: Develop and implement a communication plan to systematically relay [Transportation Worker Identification Credential] program updates to stakeholders.

Response: Concur. TSA's Enrollment Services and Vetting Programs is developing a comprehensive communication plan to systematically relay information to stakeholders. Once complete, this plan will define: a) goals and objectives; b) communication channels and schedules; c) monitoring and evaluation actions; and d) risks and mitigation actions. In September 2025, TSA also resumed Transportation Worker Identification Credential Stakeholder Communications Committee meetings as an additional avenue to share information with stakeholders, and is engaging in monthly, quarterly, and bi-annual touchpoints scheduled throughout fiscal year 2026 to ensure ongoing engagement. Further, TSA published three technical advisories¹ for self-certified technology vendors regarding Transportation Worker Identification Credential card technology and use of the credential in Physical Access Control systems. Estimated Completion Date: December 31, 2026.

GAO recommended the Commandant of the Coast Guard:

Recommendation 2: Communicate [Transportation Worker Identification Credential]-related violation and deficiency data with inspectors in the field who enforce [Transportation Worker Identification Credentials].

Response: Concur. The Coast Guard's Office of Port and Facility Compliance will develop a process or mechanism to communicate Transportation Worker Identification Credential-related violation and deficiency data with Coast Guard inspectors who enforce Transportation Worker Identification Credentials. This will include efforts such as sharing quarterly deficiency data with field personnel via an internal SharePoint site, email distributions, and/or regular conference calls with field units, as appropriate. Estimated Completion Date: March 31, 2027.

¹ TA-2024-TWIC002-V2, "Next Generation (NEXGEN) TWIC Card Issuance," dated June 28, 2024; See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwja-i-mGo-GTAXXZFkFHdnCAXeQFnoECBwQAQ&url=https%3A%2F%2Fwww.tsa.gov%2Fsites%2Fdefault%2Ffiles%2Ftechnical-advisory_twic_2024_002-v5.pdf&usq=AOvVaw26ZvXXTD3KTNimpa4nNKfN&opi=89978449.

TA-2025-TWIC001, "Change of TWIC Certificate Authority Signing Certificates," dated November 22, 2025; See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiQlb-2peGTAXUdKlKfHdyuFQEQFnoECBoQAQ&url=https%3A%2F%2Fwww.tsa.gov%2Fsites%2Fdefault%2Ffiles%2Ftwic-2025-001.pdf&usq=AOvVaw2xuUgqovUgJdQ97Cbe1BY_&cschid=177557541630543&opi=89978449.

TA-2026-TWIC001, "Notification of TWIC Cryptography Migrating to Elliptic Curve" dated January 16, 2026.

Recommendation 3: Include deficiency data in its [Transportation Worker Identification Credential] performance measure reporting.

Response: Concur. The Coast Guard's Office of Port and Facility Compliance will coordinate with the Coast Guard's Office of Program Analysis and Evaluation to ensure inclusion of Transportation Worker Identification Credential deficiency data in performance measure reporting, as appropriate. Specifically, the Coast Guard intends to include this deficiency data into existing DHS quarterly reporting. Estimated Completion Date: March 31, 2027.

Recommendation 4: Develop a method to mitigate the risks of unauthorized individuals with [Transportation Worker Identification Credential] cards on the Canceled Card List accessing secure areas of [Maritime Transportation Security Act of 2002]-regulated facilities.

Response: Concur. The Coast Guard's Office of Port and Facility Compliance will conduct a review of, and revise as appropriate, Coast Guard facility inspector guidance and procedures to mitigate the risk of unauthorized access from individuals on TSA's Cancelled Card List. This review will identify what changes are needed, if any, to address the potential risk of unauthorized individuals accessing secure areas. Estimated Completion Date: December 31, 2026.

Recommendation 5: Coordinate with TSA, through DHS, to acquire [Transportation Worker Identification Credential] reader devices for use during inspections.

Response: Concur. The Coast Guard anticipates finalizing the initial acquisition of Transportation Worker Identification Credential readers in February 2026. Following this, the Coast Guard Office of Port and Facility Compliance will coordinate with TSA, as appropriate, on future Transportation Worker Identification Credential reader acquisitions. Estimated Completion Date: December 31, 2026.

GAO recommended the TSA Administrator:

Recommendation 6: Coordinate with the Coast Guard, through DHS, to acquire [Transportation Worker Identification Credential] readers for use during inspections, as appropriate.

Response: Concur. TSA's Enrollment Services and Vetting Programs and Surface Operations offices will conduct planning for the acquisition of Transportation Worker Identification Credential card reader devices in coordination with the Coast Guard, as appropriate, to reduce program costs and enhance security operations for both DHS Components. Specifically, TSA will develop an acquisition plan, in coordination with Coast Guard, that addresses technical requirements, cost goals, and acquisition

streamlining procedures.

Since the inception of the Transportation Worker Identification Credential program, TSA and Coast Guard shared Transportation Worker Identification Credential card reader and hardware application specification information. Joint agency coordination on reader acquisitions and contracts will reinforce the security value of biometrically authenticating the Transportation Worker Identification Credential card to the cardholder. This approach will ensure active use of the Canceled Card List enhancing interoperability and consistency between TSA and the Coast Guard. Estimated Completion Date: September 30, 2026.

GAO recommended the Commandant of the Coast Guard:

Recommendation 7: Develop and implement a plan on how it will issue final regulations to specify which facilities must have [Transportation Worker Identification Credential] card readers.

Response: Concur. The Coast Guard's Office of Port and Facility Compliance and Office of Standards Evaluations and Development are currently engaged in a regulatory rule-making process for Transportation Worker Identification Credential reader regulations. Specific dates for rulemaking efforts and milestones will be published when finalized and in alignment with the policies and priorities of the current administration. Estimated Completion Date: April 30, 2027.

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

Tina Won Sherman, shermant@gao.gov

Staff Acknowledgments

In addition to the individual named above, Joy Booth (Assistant Director), Paul Hobart (Assistant Director), Robin Freshwater Nye (Analyst in Charge), Christina Lee, Stephanie Quinones Gamboa, and Makenna Slaughenhaupt made key contributions to this report. Other staff who made key contributions to the report were Lauri Barnes, Eric Hauswirth, Mary Offutt-Reagin, Amanda Panko, and Janet Temko-Blinder.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.