



**Privacy Impact Assessment Update
for the**

**Transportation Worker Identification
Credential (TWIC) Reader Requirements
for U.S. Coast Guard**

DHS/USCG/PIA-019(a)

October 9, 2015

Contact Point

**Lieutenant Commander Kevin McDonald
Program Manager, Security Standards
Branch Office of Port and Facility Activities
(CG-FAC) Cargo & Facilities Division
(CG-FAC-2)
(202) 372-1168**

Reviewing Official

**Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717**



Abstract

In January 2016, the Department of Homeland Security (DHS) United States Coast Guard (Coast Guard) will issue a Final Rule that will require owners or operators of vessels and facilities that meet certain risk factors to use, as an access control measure, electronic readers that work in combination with the Transportation Worker Identification Credential (TWIC). The Transportation Security Administration (TSA) already issues the TWIC to more than two million workers in the maritime sector and is not covered by this Privacy Impact Assessment (PIA). The Coast Guard rule will require third parties (i.e., owners or operators of certain regulated vessels and facilities) to collect limited personally identifiable information (PII) from TWIC readers. The Coast Guard has conducted this PIA in advance of the Final Rule.

Overview

The Coast Guard intends to publish a Final Rule that will require owners or operators of vessels and facilities that meet certain risk factors to use, as an access control measure, electronic readers that work in combination with the Transportation Worker Identification Credential (TWIC). The Transportation Security Administration (TSA) already issues the TWIC to more than two million workers in the maritime sector and that process is not covered by this PIA.¹ This final rule will require owners or operators whose vessels or facilities meet a certain risk threshold to conduct an “electronic TWIC inspection” whenever a person is granted unescorted access to a secure area.

Electronic TWIC inspection involves the capture of the following information when an individual’s TWIC is scanned using a TWIC reader: (1) the TWIC holder’s Federal Agency Smart Credential-Number (FASC-N); (2) the date of scan; and (3) the time of scan. Additionally, if the reader that scans the TWIC is part of a Physical Access Control System (PACS) and captures the name of the individual TWIC holder, the rule will require that that information be retained as well. This Coast Guard rulemaking will implement statutory mandates found in the Maritime Transportation Security Act (MTSA) of 2002 and the Security and Accountability For Every (SAFE) Port Act of 2006,² and is designed to improve the security of the nation’s vessels and maritime facilities.

The Coast Guard originally conducted a PIA in 2013, which analyzed the privacy risks and mitigations surrounding the proposed rule because the proposed rule will require third

¹ See DHS/TSA/PIA-012 Transportation Worker Identification Credential (TWIC) Program Final Rule PIA (October 5, 2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic09.pdf.

² See 46 U.S.C. § 70105.



parties (i.e., owners or operators of certain regulated vessels and facilities) to collect limited personally identifiable information (PII) from TWIC readers.³

The Coast Guard is updating this PIA to reflect the forthcoming Final Rule. The Final Rule is necessary to improve the security of the nation's vessels and port facilities and to comply with statutory requirements. As authorized by the MTSA, TSA established the TWIC program to address identity management shortcomings and vulnerabilities identified in the nation's transportation system. The Coast Guard promulgated regulations⁴ that require an individual to possess a TWIC before an owner or operator grants that individual unescorted access to secure areas of a MTSA-regulated vessel or facility. In order to obtain a TWIC, an individual must pay an enrollment fee and undergo a TSA security threat assessment.⁵ The SAFE Port Act further requires the Coast Guard, through delegated authority, to promulgate regulations requiring the use of TWIC readers in the maritime sector. This new rulemaking is necessary to advance the maritime security goals of the TWIC program. As described more fully below, this rule incorporates a risk-based approach to categorizing vessels and facilities based on the consequences of involvement in a severe transportation security incident, such as a terrorist attack. Vessels and facilities in the highest risk group (Risk Group A) are required to deploy TWIC readers as an access control measure. Other vessels and facilities subject to MTSA will continue to visually inspect TWICs as an access control measure.

When used as a visual identity badge, the TWIC provides a considerable security benefit because it is the single credential used throughout the maritime sector and has uniform appearance and security features. Moreover, the TWIC program ensures a vetted maritime workforce because each TWIC holder must undergo TSA's security threat assessment as part of the process of applying for and obtaining a TWIC. Although the security benefits of using a TWIC as a visual identity badge are substantial, electronic TWIC readers will provide even greater security benefits because they are more reliable than a security guard's visual inspection for verifying the identity of the TWIC holder and ensuring that the TWIC is authentic and valid.

DHS designed the TWIC to contain several enhanced security features that can only be utilized through the use of an electronic TWIC reader. One of these features is the set of two biometric templates embedded in each TWIC. An electronic TWIC reader will match the TWIC holder's biometric to one of the embedded biometric templates. This provides a more reliable form of identity verification than a visual comparison of the TWIC holder's face to the photograph on the TWIC. An electronic TWIC reader is also more reliable than visual inspection

³ DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard (March 25, 2013), available at <http://www.dhs.gov/publication/privacy-documents-us-coast-guard>.

⁴ 72 FR 3578 (January 25, 2007).

⁵ The TSA security threat assessment process is described in the privacy impact assessment DHS/TSA/PIA-012 [Transportation Worker Identification Credential Program Final Rule](http://www.dhs.gov/publication/privacy-documents-us-coast-guard) (October 5, 2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic09.pdf.



for ensuring that a TWIC is not counterfeit or expired, and can ascertain whether a TWIC has been reported lost, stolen, damaged, or revoked.

Reason for the PIA Update

The rulemaking has transitioned from an Notice of Proposed Rulemaking (NPRM) to a Final Rule, which is currently in DHS clearance and is projected to be published in the Federal Register by January 2016. There have been no substantive changes since the previous PIA was submitted with the NPRM package.

On March 22, 2013, the Coast Guard published an NPRM for this rulemaking and provided a 2-month comment period. The Coast Guard received more than 100 comment letters consisting of more than 1,200 unique comments. Additionally, the Coast Guard held four public meetings across the country in 2013.

Privacy Impact Analysis

Authorities and Other Requirements

The authorities and other requirements have not changed with this update, and no new privacy risks have been identified.

Characterization of the Information

The characterization of the information has not changed with this update, and no new privacy risks have been identified.

As described in the original PIA for the TWIC Reader Requirements,⁶ the original collection of PII for a TWIC is submitted to TSA by all credentialed merchant mariners and individuals who wish to obtain unescorted access to secure areas of a regulated facility or vessel. Information is also collected from applicants who are commercial drivers licensed in Canada or Mexico who transport hazardous materials in accordance with 49 CFR 1572.201.

TWIC readers do not collect all of the information stored on the TWIC itself. The TWIC reader will only collect the minimum amount of information necessary to verify the identity of the TWIC-holder and to validate and authenticate the credential during entry to the vessel or facility.

⁶ DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard (March 25, 2013), available at <http://www.dhs.gov/publication/privacy-documents-us-coast-guard>.



TWIC readers typically do not capture or record the name of the TWIC-holder. A TWIC reader only captures the TWIC-holder's name if it is a contact TWIC reader (i.e., one that requires the TWIC-holder to insert the TWIC into a slot for direct contact between the TWIC reader and the chip embedded in the TWIC) and only after the TWIC-holder has entered the PIN. Therefore, a TWIC reader will typically only capture three pieces of information when an individual's TWIC is scanned:

- (1) TWIC-holder's Federal Agency Smart Credential-Number (FASC-N);
- (2) Date of scan; and
- (3) Time of scan.

A "contact" TWIC reader captures the name information after the PIN has been entered. A PACS may also capture the name of the TWIC-holder. Whether or not a TWIC reader collects the TWIC-holder's name, the information collected is considered Sensitive Security Information (SSI) under 49 CFR 15.5, and must therefore be protected in accordance with 49 CFR Part 15.

The reasons for this collection are to assure compliance with TWIC reader requirements, increase security in the nation's maritime transportation system, and provide a more reliable method for verifying the identity of the TWIC-holder thus ensuring the TWIC is authentic and valid.

Of note, under the proposed rule, the Coast Guard would not collect PII directly. The proposed rule requires third parties (i.e., owners or operators of certain regulated vessels and facilities) to collect and maintain PII.

Uses of the Information

The uses of the information have not changed with this update, and no new privacy risks have been identified.

As described in the original TWIC Reader Rule PIA, the TWIC rule uses three risk factors to rank vessels and facilities by type to determine the level of TWIC requirements. These factors are the: (1) maximum consequences resulting from a terrorist attack; (2) criticality to the nation's health, economy, and national security; and (3) utility of the TWIC in reducing risk. Vessels and facilities are grouped in one of three "risk groups," based on the risk factors above. TWIC requirements for identity verification, card authentication, and card validation vary based on the assigned risk group. Only vessels and facilities in the highest risk group (Risk Group A) would be required to fulfill the three TWIC requirements by deploying TWIC readers.

Please see the original TWIC Reader Rule PIA for additional information.⁷

⁷ DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S.



Notice

On March 22, 2013, the Coast Guard published an NPRM for this rulemaking and provided a 2-month comment period. The Coast Guard received more than 100 comment letters consisting of more than 1,200 unique comments. Additionally, the Coast Guard held four public meetings across the country in 2013.

The public comments focused on three main aspects of the rule. First, they requested clarification regarding when TWIC cards must be read electronically. Second, many commenters protested the proposed requirement for TWIC use on passenger vessels as burdensome. Finally, several commenters, including large port facilities, suggested that TWICs should be able to be integrated into a facility's PACS.

As a result of the comments received both in written form as well as at public meetings, the Coast Guard made a variety of changes to the final rule. First, the Coast Guard extensively clarified when TWICs must be electronically read, and exactly what that process should entail. Additionally, Coast Guard included guidance on how electronic TWIC inspection could be implemented into a facility's PACS. Finally, Coast Guard made a variety of changes and clarifications that limited the scope of electronic TWIC inspection on vessels to focus on the highest risk burden and remove redundant inspection requirements. Other changes introduced into the final rule related to the treatment of barge fleeting facilities, clarification of language in the regulation, and further explanation of recordkeeping requirements.

Data Retention by the project

The data retention by the project has not changed with this update, and no new privacy risks have been identified.

Information Sharing

The information sharing has not changed with this update, and no new privacy risks have been identified.

Redress

Redress has not changed with this update, and no new privacy risks have been identified.



Auditing and Accountability

Auditing and accountability have not changed with this update, and no new privacy risks have been identified.

Responsible Official

Lieutenant Commander Kevin McDonald
Program Manager
Security Standards Branch Office of Port and Facility Activities (CG-FAC)
Cargo & Facilities Division (CG-FAC-2)
U.S. Coast Guard
Department of Homeland Security (202) 372-1168
Kevin.J.McDonald@uscg.mil

Approval Signature

Original signed copy on file with DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security