Privacy Impact Assessment
for the

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

DHS/USCG/PIA-019

March 25, 2013

Contact Point
Lieutenant Commander Loan O'Brien
Program Manager, Security Standards Branch
Office of Port and Facility Activities (CG-544)
Cargo & Facilities Division (CG-5422)
(202) 372-1133

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) United States Coast Guard (USCG) intends to publish a Notice of Proposed Rulemaking (NPRM) that would 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 TWIC itself has already been issued by the Transportation Security Administration (TSA) to more than two million workers in the maritime sector and is not covered by this PIA. The proposed rule would require owners or operators whose vessels or facilities meet a certain risk threshold to capture the following information when an individual's TWIC is scanned using a TWIC reader. Information captured by the TWIC readers includes: (1) the TWIC-holder's Federal Agency Smart Credential-Number (FASC-N); (2) the date of scan; (3) the time of scan; and (4) only if captured, the name of the individual TWIC-holder. 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, and is designed to improve the security of the nation's vessels and maritime facilities. This Privacy Impact Assessment (PIA) is necessary because the proposed Coast Guard rule would require third parties (*i.e.*, owners or operators of certain regulated vessels and facilities) to collect limited personally identifiable information (PII) from TWIC readers.

Overview

This proposed rulemaking is necessary to improve the security of the nation's vessels and port facilities and to comply with statutory requirements. As authorized by MTSA, TSA established the TWIC program to address identity management shortcomings and vulnerabilities identified in the nation's transportation system. The USCG has promulgated regulations (72 FR 3578, January 25, 2007) that require an individual to possess a TWIC before an owner or operator grants the 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.[1] The SAFE Port Act further requires the USCG, 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, the proposed 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

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

risk group (Risk Group A) would be required to deploy TWIC readers as an access control measure. Vessels and facilities in the two lower risk groups (Risk Groups B and C) would 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. While 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 fingerprint templates embedded in each TWIC. An electronic TWIC reader will match the TWIC-holder's fingerprint to one of the embedded fingerprint 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 for ensuring that a TWIC is not counterfeit or expired, or has not been reported lost, stolen, damaged, or revoked.

The Transportation Worker Identification Credential (TWIC)

The TWIC is a tamper-resistant biometric credential issued to eligible maritime workers who require unescorted access to secure areas of MTSA-regulated vessels and facilities.

To obtain a TWIC, applicants must provide biographic and biometric information, and complete a TSA security threat assessment. Applicants are disqualified from obtaining a TWIC if their assessment reveals that they: have been convicted, or found not guilty by reason of insanity, of certain felonies; are under want, warrant, or indictment for certain felonies; have been released from incarceration within the preceding five year period for committing certain felonies; may be denied admission to, or removed from, the United States under the Immigration and Nationality Act; or otherwise pose a terrorism security risk to the United States.

The TWIC itself shows the holder's photograph, name, and TWIC expiration date, and the back shows a unique credential number (TWIC Serial Number). In addition, the TWIC stores two electronically readable reference biometric templates (*i.e.*, fingerprint templates), a personal identification number (PIN) selected by the TWIC-holder, a digital facial image, authentication certificates, and a Federal Agency Smart Credential-Number (FASC-N). These features enable the TWIC to be used in different ways for: (1) identity verification; (2) card authentication; and (3) card validation.

(1) Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. In its most reliable form, identity verification is done by matching one of the fingerprint templates stored in the TWIC to the TWIC-holder's live sample biometric using an electronic TWIC reader. However, it can also be done with a lower level of assurance by visually comparing the photo on the TWIC to the TWIC-holder, or by requiring the TWIC-holder to place the TWIC into a TWIC reader and enter a 6- , 7-, or 8-digit PIN selected by the TWIC-holder at the time of card activation.

(2) Card authentication ensures that the TWIC is not counterfeit. The most effective method of card authentication involves using a TWIC reader to perform a challenge/response protocol using the Card Authentication Certificate (CAC) and the associated card authentication private key stored in the TWIC.[2] Alternatively, a security guard can authenticate a TWIC by visually inspecting the security features on the card, though this is a less reliable method of authentication.

(3) Card validation ensures that the TWIC has not expired or been revoked by TSA, or reported as lost, stolen, or damaged. A TSA-canceled TWIC is placed on TSA's official Canceled Card List (CCL),[3] which is updated daily. In its most reliable form, card validity is confirmed by finding no match on the CCL and a visual check of the expiration date on the TWIC. Checks against the CCL may be performed electronically by downloading the list onto a TWIC reader or a separate Physical Access Control System (PACS).[4] Card validity may be partially confirmed by visually checking the TWIC's expiration date only, though this method would not screen individuals against the CCL.

TWIC Reader Requirements

TWIC requirements vary by type of vessel and facility. The proposed rulemaking uses a risk-based approach for evaluating and categorizing types of vessels and facilities to create a framework for assigning appropriate TWIC requirements. Three risk factors are used to rank

[2] The TWIC reader will read the CAC from the card and send a command to the card requesting the card authentication key be used to sign a random block of data (created and known to the TWIC reader). The TWIC reader will use the public key embedded in the CAC to verify that the signature of the random data block is valid. If the signature is valid, the TWIC reader will trust the TWIC submitted and will then pull the Federal Agency Smart Credential-Number (FASC-N) and other information from the card for further processing. The CAC contains the FASC-N and a certificate of expiration date harmonized to the TWIC expiration date. This minimizes the need for the TWIC reader to pull more information from the card (unless required for additional checking).

[3] Invalid TWICs are placed on the CCL if they are lost, stolen, damaged, or revoked by TSA for cause. The benefit of a requirement to check TWICs against the CCL is that it enables owners and operators to limit the access to secure areas of our nation's transportation system to individuals that hold a TWIC.

[4] Physical Access Control System (PACS) means a system, including devices, personnel, and policies, that controls access to and within a facility or vessel.

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. The TWIC requirements for (1) identity verification, (2) card authentication, and (3) card validation (detailed above) vary based on the risk group.[5] Only vessels and facilities in the highest risk group (Risk Group A) would be required to fulfill all three TWIC requirements by deploying TWIC readers. Vessels and facilities in the lower risk groups would fulfill the three TWIC requirements by using the TWIC as a visual identity badge.

The risk ranking of vessels and facilities generally corresponds to the number of passengers or the hazardous nature of the cargo carried or handled. For example, a vessel certificated to carry more than 1,000 passengers is classified as high risk (Risk Group A). Similarly, a facility that handles bulk explosives, poisonous gas, or other dangerous materials is classified in Risk Group A. Because of the risks present at Risk Group A vessels and facilities, the proposed rule would require those entities to employ the TWIC's most protective measures for identity verification, card authentication, and card validation:

(1) For identity verification, owners and operators of vessels or facilities in Risk Group A would be required to either match the TWIC-holder's fingerprint to one of the fingerprint templates stored in the TWIC, or match the TWIC-holder's alternate biometric to one captured and stored in a PACS. This match would need to be made using a TWIC reader and/or PACS before the individual is granted unescorted access to secure areas.

When electronically matching biometrics within a PACS, an owner or operator would be permitted to use a different biometric than a fingerprint (*e.g.*, an iris scan or hand geometry), stored in the PACS and matched to the biometric of the TWIC-holder. The owner's or operator's system must be linked to the TWIC in such a manner that the PACS precludes access to someone who does not have a TWIC, or to someone other than the individual to whom the TWIC has been issued. This requirement means that the TWIC would need to be read and the stored biometric identifier matched against the TWIC-holder's fingerprint at least once, when the individual's information is entered into a PACS.

(2) For card authentication, owners and operators of vessels or facilities in Risk Group A would be required to use a TWIC reader to screen individuals seeking access to secure areas. As with identity verification, owners and operators would be permitted

[5] For a more detailed discussion of each risk group and the TWIC reader requirements, please refer to the USCG NPRM "Transportation Worker Identification Credential (TWIC) – Reader Requirements."

to integrate TWIC into a PACS, provided that the owner or operator completes this integration before the TWIC-holder's information is added into the PACS, and before the TWIC-holder is granted unescorted access to secure areas.

(3) For card validation, owners and operators of vessels or facilities in Risk Group A would be required to use a TWIC reader to check an individual's TWIC against the CCL. An owner or operator updates CCL information by downloading the current list onto the TWIC reader or PACS on a daily or weekly basis, depending on the MARSEC (maritime security) Level as set by the Commandant of the Coast Guard..

Recordkeeping Requirements

Before the rule is finalized, TSA will establish TWIC reader specifications and publish a Qualified Technology List (QTL) of approved TWIC readers. Owners and operators will only be allowed to use TWIC readers from the QTL to satisfy the regulatory requirements. The QTL will list a variety of types of approved TWIC readers. This will provide flexibility by enabling owners and operators to choose TWIC readers that best suit the unique needs of different vessel and facility types. Fixed TWIC readers are installed in a wall, turnstile, or similar type installation. Portable TWIC readers are hand-held. "Contactless" TWIC readers perform a scan when an individual holds a TWIC within a few inches of the device for approximately two seconds. "Contact" TWIC readers perform a scan when an individual inserts a TWIC into a slot to provide direct contact between the device and the computer chip imbedded in the TWIC. Owners and operators will have the flexibility to satisfy TWIC reader requirements by using fixed or portable readers in contact or contactless mode. Owners and operators will also have the option to integrate TWIC reader functions into an existing PACS.

When an individual's TWIC is scanned, the TWIC reader captures limited information, including the TWIC-holder's FASC-N as well as the date and time of the scan. The TWIC-holder's name would also be captured in limited circumstances, depending on the type of TWIC reader employed. For example, a TWIC reader only captures the TWIC-holder's name when operating in "contact" mode,[6] and only after the TWIC-holder enters a 6-8 digit PIN.[7] An integrated PACS may also capture the name of the TWIC-holder.

The proposed rule contains recordkeeping requirements for owners or operators using TWIC readers. Owners and operators using TWIC readers, with or without a PACS, would be required to maintain certain records for at least two years. During that time, owners and

[6] "Contact" TWIC readers perform a scan when an individual inserts a TWIC into a slot to provide direct contact between the device and the computer chip imbedded in the TWIC.

[7] The Coast Guard has observed operational challenges and limited utility associated with PIN usage. Therefore, the proposed rule would not require owners and operators to check TWIC-holder PINs. Owners and operators who wish to enhance access control would be allowed to require workers to input PIN information. However, because of the noted operational challenges and limited utility, the Coast Guard does not expect widespread PIN usage. Therefore, the Coast Guard does not expect TWIC readers to capture name information in most instances.

operators must make those records available to the Coast Guard upon request. Those records include, with respect to each individual granted unescorted access to a secure area: (1) FASC-N; (2) date that access was granted; (3) time that access was granted; and (4) if captured, the name of the individual to whom access was granted. If a TWIC reader or PACS captures the required data when the TWIC is scanned, and can retain and reproduce that data, the recordkeeping requirement would be met. Owners and operators must also maintain records to demonstrate that they have performed the required card validity check using the CCL on each individual. The proposed rule also contains a regulatory provision indicating that TWIC reader records are Sensitive Security Information (SSI), and must be protected in accordance with 49 CFR part 1520.[8]

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 102 of the Maritime Transportation Security Act (MTSA) of 2002, 46 U.S.C. § 70105 *et seq.*, requires the USCG, through delegated authority from the Secretary of Homeland Security (Secretary), to prescribe regulations to prevent an individual from entering secure areas of vessels and facilities unless the individual is so authorized and either possesses a TWIC or is escorted by someone who possesses a TWIC. Section 104 of the SAFE Port Act of 2006, supplemented MTSA by requiring the USCG, through delegated authority from the Secretary, to promulgate regulations requiring the deployment of TWIC readers in the maritime sector as part of the TWIC program.

TWIC reader recordkeeping requirements are necessary to assure compliance with the implementation of the provisions of chapter 701 of title 46 U.S.C. Section 70124 of title 46 U.S.C. authorizes the Secretary to issue regulations necessary to implement provisions of chapter 701 of title 46 U.S.C.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

[8] In accordance with 49 U.S.C. 114(s), Sensitive Security Information (SSI) is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would: (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) Reveal trade secrets or privileged or confidential information obtained from any person; or (3) Be detrimental to the security of transportation. 49 CFR part 1520 generally requires that SSI be properly marked and protected from unauthorized disclosure. Unauthorized disclosure of SSI is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

The proposed rule would require third parties (*i.e.*, owners or operators of certain regulated vessels and facilities) to potentially collect personally identifiable information. It does not allow USCG to collect any information. The System of Records Notice (SORN) DHS/TSA-002 Transportation Security Threat Assessment System, (May 19, 2010, 75 FR 28046) applies to the information maintained by the TSA for the TWIC program.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Not applicable for TWIC Reader Requirements. However, a system security plan has been completed for Transportation Worker Identification Credentials as outlined in DHS/TSA/PIA-012 Transportation Worker Identification Credential Program Final Rule.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Not applicable. Since the records are not maintained by the government, there is no records retention schedule. However, under the proposed rule recordkeeping requirements, owners and operators must maintain information collected for at least two years, and must provide the information to the USCG upon request.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Information collected by the TWIC program is covered under the PRA, TWIC Disclosure and Certification form (OMB 1652-0047).

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The original collection of personally identifiable information for a TWIC is submitted to the TSA by all credentialed merchant mariners and individuals who wish to obtain unescorted access to secure areas of a regulated facility or vessel.[9] Information is also collected from

[9] For a detailed description of all personally identifiable information collected by the TSA as part of the TWIC

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.

The proposed 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.[10] 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.

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 SSI under 49 CFR 15.5, and must therefore be protected in accordance with 49 CFR Part 15.[11]

---

enrollment process, please see DHS/TSA/PIA-012 Transportation Worker Identification Credential Program Final Rule (October 5, 2007).

[10] For a more detailed discussion of each risk group and the TWIC reader requirements, please refer to the USCG NPRM "Transportation Worker Identification Credential (TWIC) – Reader Requirements."

[11] 49 CFR Part 15 imposes duties on "certain covered" persons to protect SSI. "Covered persons" include, among others: (1) each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law; (2) each owner or operator of a maritime facility required to have a security plan under MTSA and each person who has access to SSI, as specified in 49 CFR 15.11. Furthermore, the International Ship and Port Facility Security Code requires a vessel's security plan and applicable security records to be protected from unauthorized access or disclosure. SSI information collected by a TWIC

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 USCG 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.

2.2 What are the sources of the information and how is the information collected for the project?

Information collected and maintained by the TWIC reader is a small portion of the information submitted during the TWIC enrollment process, and the time and date that the TWIC-holder accessed a vessel or facility. This information is collected directly from the individual TWIC-holders. Sources of information include all credentialed merchant mariners and individuals who wish to obtain unescorted access to secure areas of a regulated facility or vessel, and commercial drivers licensed in Canada or Mexico who transport hazardous materials in accordance with 49 CFR 1572.201.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No, TWIC readers do not use commercial or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Any PII collected by TWIC readers is based on the original information submitted during the TWIC enrollment process, and the time and date that the TWIC-holder accessed a vessel or facility. Information submitted during the TWIC enrollment process is voluntarily provided by the applicant. Information is submitted in person by the applicant to the TSA enrollment personnel, who will input the data in an electronic format. The applicant will review the data entered for accuracy before it is transmitted.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that electronic TWIC readers collect more information than is necessary to complete mission goals.

---

reader falls under that requirement.

Mitigation: The proposed 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.[12] 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.

Before the rule is finalized, TSA will establish TWIC reader specifications and publish a Qualified Technology List (QTL) of approved TWIC readers. Owners and operators will only be allowed to use TWIC readers from the QTL to satisfy the regulatory requirements. The Coast Guard expects that TSA-approved TWIC readers will not collect more information than is necessary to validate and authenticate the TWIC.

Owners and operators will also have the option to integrate TWIC reader functions into an existing PACS. In the event that more information is collected than is necessary to complete mission goals, the proposed rule contains a provision that specifically requires owners and operators integrating TWIC reader functions into a PACS to formally describe how they will protect personal information collected.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

There are two types of TWIC readers that may be used to verify the user's TWIC:

(1) Fixed Reader – a stationary TWIC reader installed in a wall, turnstile or similar type installation. It may communicate with an owner's or operator's access control system to control a door, gate, turnstile, etc. Fixed TWIC readers may operate in indoor environments or in outdoor environments exposed to the weather.

(2) Portable Reader – a handheld TWIC reader may operate in indoor environments or in outdoor environments exposed to the weather.

A TWIC may also be verified using contact smart card readers attached to a personal computer in an office environment for such functions as privilege granting, registration into a

[12] For a more detailed discussion of each risk group and the TWIC reader requirements, please refer to the USCG NPRM "Transportation Worker Identification Credential (TWIC) – Reader Requirements."

physical access control system and for logical access control. This PIA only describes TWIC readers that shall be used for physical access into a facility or vessel.

The PII stored on the TWIC enables the TWIC reader to be used in different ways for: (1) identity verification; (2) card authentication; and (3) card validation.

(1) Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. In its most reliable form, identity verification is done by matching one of the fingerprint templates stored in the TWIC to the TWIC-holder's live sample biometric using an electronic TWIC reader. However, it can also be done with a lower level of assurance by visually comparing the photo on the TWIC to the TWIC-holder, or by requiring the TWIC-holder to place the TWIC into a TWIC reader and enter a 6- , 7-, or 8-digit PIN selected by the TWIC-holder at the time of card activation.

(2) Card authentication ensures that the TWIC is not counterfeit. The most effective method of card authentication involves using a TWIC reader to perform a challenge/response protocol using the Card Authentication Certificate (CAC) and the associated card authentication private key stored in the TWIC.[13] Alternatively, a security guard can authenticate a TWIC by visually inspecting the security features on the card, though this is a less reliable method of authentication.

(3) Card validation ensures that the TWIC has not expired or been revoked by TSA, or reported as lost, stolen, or damaged. A TSA-canceled TWIC is placed on TSA's official Canceled Card List (CCL),[14] which is updated daily. In its most reliable form, card validity is confirmed by finding no match on the CCL and a visual check of the expiration date on the TWIC. Checks against the CCL may be performed electronically by downloading the list onto a TWIC reader or a separate Physical Access Control System (PACS).[15] Card validity may be partially confirmed by visually checking the TWIC's expiration date only, though this method would not screen individuals against the CCL.

[13] The TWIC reader will read the CAC from the card and send a command to the card requesting the card authentication key be used to sign a random block of data (created and known to the TWIC reader). The TWIC reader will use the public key embedded in the CAC to verify that the signature of the random data block is valid. If the signature is valid, the TWIC reader will trust the TWIC submitted and will then pull the Federal Agency Smart Credential-Number (FASC-N) and other information from the card for further processing. The CAC contains the FASC-N and a certificate of expiration date harmonized to the TWIC expiration date. This minimizes the need for the TWIC reader to pull more information from the card (unless required for additional checking).

[14] Invalid TWICs are placed on the CCL if they are lost, stolen, damaged, or revoked by TSA for cause. The benefit of a requirement to check TWICs against the CCL is that it enables owners and operators to limit the access to secure areas of our nation's transportation system to individuals that hold a TWIC.

[15] Physical Access Control System (PACS) means a system, including devices, personnel, and policies, that controls access to and within a facility or vessel.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, the TWIC reader project does not use technology to conduct electronic searches to discover or locate a predictive pattern or anomoly.

3.3 Are there other components with assigned roles and responsibilities within the system?

TSA is the lead component within DHS for the TWIC program. The role of the USCG in proposing the new TWIC reader requirements rule is to improve the security of the nation's vessels and port facilities and to comply with statutory requirements.

TSA collects the PII directly from individuals applying for a TWIC, enrolls approved applicants into the TWIC program, and issues the physical credential to the TWIC-holder. TSA is also the point of contact for TWIC-holders who have redress questions or concerns regarding their credential. Additionally, TSA and the Department of Commerce's National Institute of Standards and Technology (NIST) are developing TWIC reader specifications. TSA will establish a process to qualify TWIC readers, and maintain a Qualified Technology List (QTL) of acceptable TWIC readers.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that that information collected by the TWIC readers will be used inconsistent with the maritime security mission goals.

Mitigation: The existing regulations that would apply to the TWIC reader recordkeeping requirements specifically require that any records must be protected from unauthorized access or disclosure (33 CFR 104.235(c); 33 CFR 105.225(c)). Additionally, violators would be subject to 33 CFR 101.410, which authorizes the Coast Guard Captain of the Port to impose a broad range of control, compliance, and corrective measures. Violators would also be subject to the civil penalties in 33 CFR 101.415(b), which impose liability of up to $25,000 per violation.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

When an individual applies for a TWIC at the TSA enrollment center, applicants receive a Privacy Act Statement and consent form, by which they agree to provide PII for the security threat assessment and credential. For applicants who pre-enroll, the Privacy Act Statement is provided with the application online, but the applicants must acknowledge receipt of the notice in writing at the enrollment center. If an applicant fails to sign the consent form or does not have the required documents to authenticate identity, enrollment will not proceed. All information collected at the enrollment center or during the pre-enrollment process, including the signed Privacy Act Statement and consent form and identity documents are scanned into the TSA system for storage. All PII is encrypted or hashed to protect the information from unauthorized retrieval or use. TSA's Privacy Impact Assessment, DHS/TSA/PIA-012 Transportation Worker Identification Credential Program Final Rule (October 5, 2007) and the associated Final Rule also served to provide notice of the above. The applicable Privacy Act System of Records Notice (SORN), DHS/TSA-002, Transportation Security Threat Assessment Systems (T-STAS) was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731-67735.

If a TWIC is lost, stolen, or damaged, individual TWIC-holders must contact the TSA for assistance. The TSA maintains the "Canceled Card List," which is the list of TWIC Federal Agency Smart Credential-Numbers that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or because the card has been reported lost, stolen, or damaged.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Applicants provide information voluntarily to TSA and individuals who do not provide the information will be ineligible to receive a TWIC. Therefore, they would not have unescorted access authority to secure areas of facilities and vessels. SSN is a voluntary item of information. For individuals who choose to refuse to provide a SSN, such refusal may result in delays in processing their application and completing the security threat assessment.

Once a TWIC has been issued, if a TWIC reader is in place at a vessel or facility, TWIC-holders must use the TWIC reader to enter the facility.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that that notice may not been adequately provided to individuals prior to obtaining a TWIC.

Mitigation: Prior to the TWIC compliance date of April 15, 2009 (regarding the requirement on workers to obtain a TWIC), TSA and Coast Guard worked closely with industry to inform the public of the TWIC requirements. These information and guidance documents are still available at the Coast Guard's internet site in Homeport as well as TSA's TWIC Internet site. In addition, the Coast Guard and TSA also have TWIC Help Desks for individuals to call and/or send e-mails on TWIC issues.

Privacy Risk: There is a risk that TWIC-holders will not be notified of what information is stored on TWIC readers and what third parties have access to the information.

Mitigation: Owners and operators would work closely with affected TWIC-holder population on how to use the TWIC with the TWIC readers and inform the users on what information is stored on TWIC readers. In addition, the public is notified that TWIC information is passed to third parties through this PIA and applicable Routine Use (N) in DHS/TSA-002, Transportation Security Threat Assessment Systems (T-STAS): "to airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers and other facility operators about individuals who are their employees, job applicants or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, training or the issuance of such credentials or clearances."

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The proposed rule would require owners and operators of certain regulated vessels and facilities to collect and maintain the TWIC reader data elements for at least two years, and provide this information to the USCG upon request.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information within the TWIC reader will be retained for longer than necessary to accomplish the purpose for which the information was originally collected.

Mitigation: The information in TWIC readers will be retained for the timeframes outlined in Question 5.1 to allow USCG and TSA to properly carry out the dissemination, collaboration, and validation purposes for which the information was originally collected. The proposed rule contains provisions that emphasize this information is designated as SSI.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes, the information originally collected by the TSA as part of the TWIC credentialing process is shared with the owners or operators, whose vessels or facilities meet a certain risk threshold, when an individual's TWIC is scanned using a TWIC reader. The proposed rule would require owners or operators of certain MTSA-regulated vessels and facilities using electronic TWIC readers to capture and retain records for two years the following four pieces of information when an individual's TWIC is scanned using a TWIC reader: (1) TWIC-holder's Federal Agency Smart Credential—Number; (2) date of scan; (3) time of scan; and (4) only if captured, the name of the individual TWIC-holder. Under the proposed rule, the Coast Guard would not collect PII. The proposed rule would require third parties (*i.e.*, owners/operators of certain regulated vessels and facilities) to potentially collect PII.

PII may also be collected by the owners or operators without the use of a TWIC reader. Owners and operators may develop written log files to account for the visual inspections of TWICs as part of their normal facility and vessel access control procedures, though this is not required by the proposed rule.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

When an individual presents his/her TWIC, the individual is providing consent to the owner's or operator's collection and maintenance of the information maintained on the TWIC discussed above. Additionally, consistent with the System of Records Notice, DHS/TSA-002, Transportation Security Threat Assessment Systems (T-STAS) (May 19, 2010, 75 FR 28046), information may be shared outside of the Department under Routine Use (N): "To airport operators, aircraft operators, maritime and surface transportation operators, indirect air carriers and other facility operators about individuals who are their employees, job applicants or contractors, or persons to whom they issue identification credentials or grant clearances to

secured areas in transportation facilities when relevant to such employment, application, contract, training or the issuance of such credentials or clearances."

6.3 Does the project place limitations on re-dissemination?

Yes. Owners and operators who collect and maintain the TWIC reader data cannot share this information outside of their vessel or facility. The only allowable sharing is back to the TSA or the USCG for auditing or law enforcement purposes, or to assist with customer redress.

Owners and operators are also bound by the restrictions on disclosure of SSI (49 CFR 15.9(a)(1)). Unauthorized disclosure of SSI is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure. Covered persons who handle SSI have a duty to protect information and are required to take reasonable steps to safeguard SSI from unauthorized disclosure. When not in physical possession of SSI, covered persons are required to store it in a secure container, such as a locked desk or file cabinet or in a locked room. Disclosure of SSI can only be made to covered persons who have a need to know.

Additionally, the existing regulations that would apply to the TWIC reader recordkeeping requirements specifically require that any records must be protected from unauthorized access or disclosure (33 CFR 104.235(c); 33 CFR 105.225(c)). Violators would be subject to 33 CFR 101.410, which authorizes the Coast Guard Captain of the Port to impose a broad range of control, compliance, and corrective measures. Violators would also be subject to the civil penalties in 33 CFR 101.415(b), which impose liability of up to $25,000 per violation.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Owners/operators that are required to install and use TWIC readers must submit a Vessel Security Plan or Facility Security Plan amendment to the Marine Safety Center, cognizant Captain of the Port, or District Commander in accordance with 33 CFR 104.415(a), 105.415(a), or 106.415(a). The amendment must detail the implementation of a TWIC reader system as an equivalent access control procedure to the one established by 33 CFR 104.265(c)(1), 105.255(c)(1), or 106.260(c)(1), as applicable.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information contained on a TWIC reader may be shared outside the Department inconsistent with maritime security mission needs.

Mitigation: To minimize the amount of PII transferred from the TWIC to the TWIC reader, they will be specifically designed to only collect the minimum amount of information necessary to assist in access control and maritime security. Owners and operators who collect

and maintain the TWIC reader data cannot share this information outside of their vessel or facility. The only allowable sharing is back to the TSA or the USCG for auditing or law enforcement purposes, or to assist with customer redress.

Owners and operators are also bound by the restrictions on disclosure of SSI (49 CFR 15.9(a)(1)). Unauthorized disclosure of SSI is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

For information maintained on the TWIC, individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by email at FOIA.TSA@dhs.gov. The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/research/foia/index). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If a TWIC is lost, stolen, or damaged, individual TWIC-holders must contact the TSA for assistance. The TSA maintains the “Canceled Card List,” which is the list of TWIC Federal Agency Smart Credential-Numbers that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or because the card has been reported lost, stolen, or damaged.

If TWIC-holders have difficulty with their credential, they should contact the TWIC Program Help Desk: 1-866-DHS-TWIC (1-866-347-8942). TWIC-holders may also email the TWIC Help Desk regarding any questions about the TWIC program or TWIC status, after checking online, email the Help Desk directly at twic.helpdesk@lmbps.com. TWIC-holders should be prepared to include full name that was used at enrollment, date of birth, and application ID to allow for timely processing of their request.

7.3 How does the project notify individuals about the procedures for correcting their information?

TWIC-holders must contact the TSA to correct or update their information on file with the TWIC Program Office. TWIC-holders may contact the TSA TWIC Program Office at 1-866-DHS-TWIC (1-866-347-8942) or twic.helpdesk@lmbps.com. Additional information is available at http://twicinformation.tsa.dhs.gov/twicinfo/index.jsp.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals are not able to correct information on the TWIC.

Mitigation: The Coast Guard works closely with TSA to ensure accurate and updated TWIC information and guidance documents are available to individuals. If the information on TWIC is not accurate or not working, the individual may contact the Coast Guard or TSA TWIC program offices either via the TWIC Help Desks (by phone or e-mail) or directly with the TWIC program representatives.

The proposed rule contains provisions that address exception processing in scenarios when a TWIC reader malfunctions or when an individual's TWIC is lost, stolen, or damaged. If an individual is unable to present a TWIC because it has been lost, damaged, or stolen, and the individual has previously been granted unescorted access to secure areas and is known to have previously possessed a TWIC, an owner or operator may grant the individual unescorted access to secure areas for a period of no longer than seven consecutive days. Additionally, the individual must report the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f). The individual must also present another identification credential issued by a recognized authority, and there must be no suspicious circumstances associated with the individual's claim. The rule proposes similar relief when a TWIC reader malfunctions. This will enable business continuity while the special circumstance is remedied.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The proposed rule would require owners or operators of certain MTSA-regulated vessels and facilities to collect TWIC reader information in order to ensure that the only individuals granted access to secure areas of the nation's maritime transportation system are those that posses a TWIC. USCG inspectors would periodically inspect TWIC reader records to assure compliance with TWIC reader requirements.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

While no specific privacy training exists for owners and operators, existing regulations (33 CFR 104.200; 33 CFR 105.200) require the owner or operator to define the security organizational structure and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations. Each vessel and facility must have a designated Company Security Officer, Vessel Security Officer, and/or Facility Security Officer, as appropriate, with responsibility to ensure TWIC programs are in place and implemented properly (33 CFR 104.210; 33 CFR 104.215; 33 CFR 105.205).

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The proposed rule would place requirements on owners and operators of vessels and facilities in Risk Group A to use TWIC readers as part of their TWIC program. Existing regulations (33 CFR 104.200; 33 CFR 105.200) require the owner or operator to define the security organizational structure and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations. Each vessel and facility must have a designated Company Security Officer, Vessel Security Officer, and/or Facility Security Officer, as the case may be, with responsibility to ensure TWIC programs are in place and implemented properly (33 CFR 104.210; 33 CFR 104.215; 33 CFR 105.205). Thus, under the proposed rule, primary responsibility for TWIC reader implementation for Risk Group A would fall to the owner/operator and the security officers.

Among the duties of the owner/operator and security officers includes the protection of TWIC reader records as SSI. Accordingly, these individuals are bound by the restrictions on disclosure of SSI (49 CFR 15.9(a)(1)). Specifically, they have a duty to protect information, which requires them to take reasonable steps to safeguard SSI from unauthorized disclosure. When not in physical possession of SSI, they are required to store it in a secure container, such

as a locked desk or file cabinet or in a locked room. Disclosure of SSI can only be made to "covered persons" who have a need to know.

Additionally, the existing regulations that would apply to the TWIC reader recordkeeping requirements specifically require that any records must be protected from unauthorized access or disclosure (33 CFR 104.235(c); 33 CFR 105.225(c)). Violators would be subject to 33 CFR 101.410, which authorizes the Coast Guard Captain of the Port to impose a broad range of control, compliance, and corrective measures. Violators would also be subject to the civil penalties in 33 CFR 101.415(b), which impose liability of up to $25,000 per violation.

While security officers may assign security duties to other personnel, the security officers retain responsibility for these duties.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Information collected and stored within the electronic TWIC readers will not be shared under any information sharing access agreements. The only allowable sharing is back to the TSA or the USCG for auditing or law enforcement purposes, or to assist with customer redress.

Responsible Officials

Lieutenant Commander Loan O'Brien
Program Manager, Security Standards Branch
Office of Port and Facility Activities (CG-544)
Cargo & Facilities Division (CG-5422)
U.S. Coast Guard
Department of Homeland Security
(202) 372-1133
Loan.T.O'Brien@uscg.mil

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security