Proposed Rules

Federal Register
Vol. 74, No. 58
Friday, March 27, 2009

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 101, 104, 105, and 106

[Docket No. USCG–2007–28915]

RIN 1625–AB21

Transportation Worker Identification Credential (TWIC)—Reader Requirements

AGENCY: Coast Guard, DHS.

ACTION: Advanced notice of proposed rulemaking.

SUMMARY: This advanced notice of proposed rulemaking discusses the United States Coast Guard's preliminary thoughts on potential requirements for owners and operators of certain vessels and facilities regulated by the Coast Guard under 33 CFR chapter I, subchapter H, for use of electronic readers designed to work with Transportation Worker Identification Credentials (TWIC) as an access control measure. It discusses additional potential requirements associated with TWIC readers, such as recordkeeping requirements for those owners or operators required to use an electronic reader, and amendments to security plans previously approved by the Coast Guard to incorporate TWIC requirements.

This rulemaking action, once final, would enhance the security of ports and vessels by ensuring that only persons who hold valid TWICs are granted unescorted access to secure areas on vessels and port facilities. It would also complete the implementation of the Maritime Transportation Security Act of 2002 transportation security card requirement, as well as the requirements of the Security and Accountability for Every Port Act of 2006, for regulations on electronic readers for use with Transportation Worker Identification Credentials.

DATES: Comments and related material must reach the Docket Management Facility on or before May 26, 2009.

ADDRESSES: You may submit comments identified by Coast Guard docket number USCG–2007–28915 to the Docket Management Facility at the U.S. Department of Transportation. Please note the new address. *See* 72 FR 28092, May 18, 2007. To avoid duplication, please use only one of the following methods:

(1) *Online: http://www.regulations.gov*.

(2) *Mail:* Docket Management Facility (M–30), U.S. Department of Transportation, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue, SE., Washington, DC 20590–0001.

(3) *Hand delivery:* Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

(4) *Fax:* 202–493–2251.

(5) For comments containing confidential information, business information or sensitive security information, please mail appropriately marked comments to LCDR Jonathan Maiorine, Commandant (CG–544) (RM 5222), U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593.

FOR FURTHER INFORMATION CONTACT: If you have questions on this advanced notice of proposed rulemaking, call LCDR Jonathan Maiorine, Coast Guard, telephone 1–877–687–2243.

If you have questions on viewing or submitting material to the docket, call Renee V. Wright, Program Manager, Docket Operations, telephone 202–366–9826.

SUPPLEMENTARY INFORMATION:

Table of Acronyms

AHP Analytical Hierarchy Process
ANPRM Advanced Notice of Proposed Rulemaking
ASPs Alternative Security Programs
TWIC Transportation Worker Identification Credential
CDC Certain Dangerous Cargoes
CI/KR Critical Infrastructure/Key Resource
CRL Certificate Revocation List
DHS Department of Homeland Security
DOT Department of Transportation
EOA Early Operational Assessment
FASC–N Federal Agency Smart Credential—Number
FOIA Freedom of Information Act
FR Final Rule
FSP Facility Security Plan
HSI Homeland Security Institute
ITEP Integrated Test and Evaluation Program
ITT Initial Technical Test
MARSEC Maritime Security
MERPAC Merchant Marine Personnel Advisory Committee
MODU Mobile Offshore Drilling Unit
MSRAM Maritime Security Risk Analysis Model
MTSA Maritime Transportation Security Act
NMSAC National Maritime Security Advisory Committee
NPRM Notice of Proposed Rulemaking
OCS Outer Continental Shelf
OMB Office of Management and Budget
OSVs Offshore Supply Vessels
PACS Personnel Access Control System
PIN Personal Identification Number
PIV Personal Identity Verification
RA Regulatory Analysis
RKB Responder Knowledge Base
SSI Sensitive Security Information
ST&E System Test & Evaluation
TEMP Test and Evaluation Master Plan
TSA Transportation Security Administration
TSAC Towing Safety Advisory Committee
TSI Transportation Security Incident
TWIC Transportation Worker Identification Credential
VSP Vessel Security Plan

Table of Contents

I. Public Participation and Request for Comments

We encourage you to participate in this rulemaking by submitting

comments and related materials. All comments received will be posted, without change, to *http://www.regulations.gov* and will include any personal information you have provided. We have an agreement with the Department of Transportation (DOT) to use the Docket Management Facility.

A. Submitting Comments

If you submit a comment, please include your name and address, identify the docket number for this rulemaking (USCG–2007–28915), indicate the specific section of this document to which each comment applies, and give the reason for each comment. You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**; but please submit your comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period. We may change the proposed rule in view of them.

B. Handling Confidential Information, Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI) [1] to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the Coast Guard point of contact listed in the **FOR FURTHER INFORMATION CONTACT** section.

Upon receipt of such comments, the Coast Guard will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. The Coast Guard will hold them in a separate file to which the public does not have access, and place a note in the public docket that Coast Guard has received such materials from the commenter. If the Coast Guard receives a request to examine or copy this information, we will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552).

C. Viewing Comments and Documents

To view comments, as well as documents mentioned in this preamble as being available in the docket, go to *http://dms.dot.gov* at any time, enter the docket number for this rulemaking (USCG–2007–28915) in the Search box, and click ''Go >>.'' If you do not have access to the internet, you may view the docket online by visiting the Docket Management Facility in Room W12–140 on the ground floor of the Department of Transportation West Building, 1200 New Jersey Avenue, SE., Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

D. Privacy Act

Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review a Privacy Act, system of records notice regarding our public dockets in the January 17, 2008 issue of the **Federal Register** (73 FR 3316).

E. Public Meeting

Because the Coast Guard intends to hold additional public meetings (*see* Paragraph F ''Future Opportunities for Comment''), we plan to hold only one public meeting in the Washington, DC area at this time. A notice with the specific date and location of the meeting will be published in the **Federal Register** as soon as this information is known. In addition, known interested parties will be contacted via mail, e-mail, or telephone. If you wish to be contacted regarding the public meeting, contact LCDR Jonathan Maiorine, listed under **FOR FURTHER INFORMATION CONTACT**.

F. Future Opportunities for Comment

The Coast Guard intends to publish a Notice of Proposed Rulemaking (NPRM) after reviewing the comments on this Advanced Notice of Proposed Rulemaking (ANPRM), and after receiving data from the TWIC pilot programs (discussed in Section IV ''Discussion of Pilot Programs''). We intend to have an open comment period with sufficient time to allow interested parties to submit comments following publication of an NPRM. We also intend to hold several public meetings during that comment period, at various locations across the country.

II. Summary of ANPRM

This ANPRM presents preliminary thoughts of the Department of Homeland Security, through the U.S. Coast Guard and the Transportation Security Administration, on potential requirements for electronic TWIC readers for certain vessels and facilities that are regulated by the Coast Guard under 33 CFR chapter I, subchapter H, commonly known as ''MTSA-regulated'' vessels and facilities. The purpose of this ANPRM is to open the public dialogue on implementing TWIC reader requirements using a risk-based decision model, as well as to seek input on other requirements that we are considering proposing at the same time as the reader requirements. We are not proposing any specific changes to the Code of Federal Regulations at this time. Specific changes would be proposed in an NPRM at a future date.

This ANPRM discusses separating individual MTSA-regulated vessels, facilities, and Outer Continental Shelf (OCS) facilities into one of three risk groups. Each risk group would have its own associated electronic TWIC reader requirements.

We are considering that those vessels and facilities in the lowest risk group continue to use TWICs primarily as a visual identity badge only, at all Maritime Security (MARSEC) Levels, and subject to electronic verification during inspections and spot checks, as currently required in the joint Coast Guard and TSA final rule on TWIC, issued on January 25, 2007. 72 FR 3492.

At MARSEC Level 1, those in the middle risk group would perform an electronic read of the TWIC to verify its authenticity and to verify the validity of the card (*i.e.,* ensure that it has not been revoked). Owners or operators of these vessels and facilities would match the TWIC-holder's fingerprint to the biometric template stored within the TWIC (*i.e.*, perform a biometric match) at MARSEC Level 1 on dates chosen randomly within a frequency of at least once a month. They would perform the biometric match at each entry at the higher MARSEC Levels.

Those vessels and facilities falling into the highest risk group would perform the biometric match and verify the authenticity and validity of the card at each entry at all MARSEC Levels.

These requirements are summarized in a table, found in Section IV. D. ''Reader Requirements'' and are subject to change based on public comment and

[1] ''Sensitive Security Information'' or ''SSI'' is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

additional data collection from the TWIC reader testing pilot program (''pilot program''), which is currently underway as required by the Safety and Accountability for Every Port Act of 2006 (SAFE Port Act), Public Law No. 109–347, 120 Stat. 1884, 1889 (Oct. 13, 2006). For example, we may propose, in an NPRM, to require reader usage at a facility or vessel in Risk Group C, or require more frequent reader usage for those facilities and vessels in Risk Group B. We request comments from the public regarding this process and, in particular, the Risk Group divisions and application of MARSEC Levels to reader requirement frequency.

We are also considering that each risk group have the option of using recurring unescorted access for up to 14 TWIC holders, per vessel or facility, if that provision is included in their amended security plan and approved by the Coast Guard. In order to take advantage of recurring unescorted access, the owner or operator of the vessel or facility would conduct an initial biometric match of the individual against his/her TWIC, either at hiring or upon the effective date of a final rule, whichever occurs later. This biometric match would include a verification of the authenticity and validity of the TWIC. Once this check is done, the TWIC need only be used as a visual identity badge, at a frequency to be approved by the Coast Guard in the amended security plan, so long as the validity of the TWIC is verified periodically, ranging from monthly to daily, depending upon risk group and MARSEC Level. We are specifically seeking comment in this ANPRM as to whether 14 persons is the appropriate number of persons eligible for recurring unescorted access and whether the public believes this process is appropriate for facilitating industry operations while maintaining an appropriate level of port security.

This ANPRM also discusses recordkeeping requirements for those risk groups required to use readers, and for those owners or operators choosing to use recurring unescorted access. It discusses and seeks comment on a requirement for all owners and operators to amend their security plans to incorporate TWIC requirements.

III. Background

A. Statutory History

The principal statutory authority for the TWIC program, the Maritime Transportation Security Act of 2002 (MTSA), Public Law No. 107–295, 116 Stat. 2064 (Nov. 2, 2002), requires the issuance of biometric transportation security cards to Coast Guard credentialed merchant mariners and other workers requiring unescorted access to secure areas of vessels and port facilities. 46 U.S.C. 70105(a)–(f) (2002). The SAFE Port Act, Public Law No. 109–347, 120 Stat. 1884 (Oct. 13, 2006) supplemented various MTSA credentialing requirements. These additional provisions included establishing a port implementation deadline; requiring implementation of a pilot program to test TWIC readers; and setting a deadline for promulgation of final regulations requiring the deployment of TWIC readers that are consistent with the findings of the pilot program. 46 U.S.C. 70105(g)–(m) (2006).

B. Regulatory History

On May 22, 2006, the Coast Guard and TSA issued a joint notice of proposed rulemaking (TWIC 1 NPRM) entitled ''Transportation Worker Identification Credential Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License,'' setting forth proposed requirements and processes required by MTSA. 71 FR 29396. The TWIC 1 NPRM proposed amending Coast Guard regulations on vessel and facility security, found in 33 CFR chapter I, subchapter H, to require the use of the TWIC as an access control measure, as well as amendments to TSA regulations on security threat assessment standards. The TWIC 1 NPRM also proposed requiring the use of TWIC in a biometric access control system and user fees for TWIC issued under this rule. The joint final rule (TWIC 1 FR), issued January 25, 2007, under the same title, established the biometric credential requirements, amended knowledge requirements, expanded appeal and waiver provisions, and set the user fee for the TWIC. 72 FR 3492. The TWIC 1 FR did not require card readers. A full discussion of the provisions for the TWIC 1 NPRM and TWIC 1 FR can be found in the preambles of those documents, at the **Federal Register** cites provided in this paragraph.

After publication of the TWIC 1 FR, the Coast Guard issued a Notice of Availability and requested comments on draft TWIC biometric reader specifications and draft TWIC contactless smart card applications, which were both developed by the National Maritime Security Advisory Committee (NMSAC). The Coast Guard and TSA reviewed the comments received and issued a Notice on September 20, 2007, announcing the working technical specification selected for use in the TWIC pilot programs and discussing the comments received in response to the Notice of Availability. 72 FR 53784.

On July 13, 2007, the Coast Guard issued a final rule to delay the compliance date for facility owners and operators wishing to redefine their secure areas, to limit application of the TWIC requirement to those portions of their facility directly connected to maritime transportation. 72 FR 38486. This provision was included in the TWIC 1 FR, and the delay in the compliance date was necessary to allow owners and operators to consider Coast Guard guidance, issued as Navigation and Vessel Inspection Circular 03–07 on July 2, 2007.

On September 28, 2007, the Coast Guard and TSA issued another joint Final Rule to amend provisions of the TWIC 1 FR. 72 FR 55043. This final rule amended the definition of secure areas to address facilities in the Commonwealth of the Northern Mariana Islands; allowed flexibility for additional non-resident aliens to apply for a TWIC; clarified who may obtain a TWIC at a reduced fee; and amended the replacement fee originally announced in TWIC 1 FR.

On May 7, 2008, the Coast Guard and TSA issued a joint final rule to extend the compliance date set forth in the TWIC 1 FR. 73 FR 25562. Under the new final compliance date, mariners must obtain a TWIC no later than April 15, 2009. That date also marks the final date by which owners and operators of vessels, facilities, and OCS facilities, who have not otherwise been required to implement access control procedures utilizing TWIC on an earlier date, must implement those procedures. Owners and operators of vessels, facilities, and OCS facilities should note, however, that in accordance with the TWIC 1 FR the Coast Guard has announced rolling COTP Zone compliance dates in the **Federal Register**.

IV. Discussion of Process

A. Risk-Based Approach to Reader Requirements

This ANPRM discusses three levels of requirements, with vessels and facilities ''assigned'' into a particular level based on risk. We used the Maritime Security Risk Analysis Model (discussed in B. ''Maritime Security Risk Analysis Model (MSRAM) and the Analytic Hierarchy Process (AHP)'') and other factors to rank facilities and vessels as lower versus higher risk. We are considering proposing that those facilities and vessels with the higher risk be required to fully utilize the security features and achieve the full risk reduction benefit of the TWIC, whereas facilities and vessels

at the lower risk level should be required to implement only some of the security features. We have presented the resulting matrix of potential requirements in this document. We are seeking comment not only on these requirements, but also on the risk groups themselves and the method we used to reach those groups, which is discussed in the next section.

B. Maritime Security Risk Analysis Model (MSRAM) and the Analytic Hierarchy Process (AHP)

Three factors were applied to develop a risk-based ranking of all MTSA-regulated facilities and vessels by type. These factors were: The maximum consequence resulting from a terrorist attack, the criticality to the nation's health, economy and national security, and the utility of TWIC in reducing risk. These factors were applied in an AHP (discussed later in this section) to develop an overall ranking of vessel and facility types for which TWIC requirements are assigned.[2]

The first factor applied was the maximum potential consequence resulting from the total destruction of the vessel or facility. We developed this factor by using the Coast Guard's MSRAM application.

MSRAM is a terrorism risk analysis tool used to perform risk assessments on critical infrastructure and key resources in the maritime domain given a range of terrorist attack scenarios. The tool's purpose is to capture and rank the security risk facing different types of potential terrorist targets (*e.g.*, waterfront facilities, vessels, bridges and other infrastructure) spanning all Critical Infrastructure/Key Resource (CI/KR) sectors in our nation's ports and on our waterways. An initial step in the MSRAM process is to calculate the maximum potential consequence of total loss of a target, factoring in injury and loss of life, economic and environmental impact, symbolic effect, and national security impact. MSRAM then assesses risk for a range of scenarios—each involving a combination of target and method of attack—in terms of threat, vulnerability, and consequence. MSRAM also considers the response capability of the owner/operator, local first responders, and Federal agencies to mitigate the consequences of an attack. The Coast Guard in consultation with representatives from Area Maritime Security Committees throughout the country has compiled this MSRAM risk information from Coast Guard Sectors and Captains of the Port into a database which provides an overall national view of terrorist risk to maritime assets.

We extracted information specific to MTSA regulated vessels and facilities from this database and used it to address the maximum consequence that would occur if the facility or vessel was completely debilitated by a transportation security incident (TSI) resulting from a terrorist attack. These MSRAM consequence scores were averaged across similar types of MTSA regulated vessels and facilities to develop a standard risk score for each type of vessel and facility.

The second factor scored was the criticality of vessel or facility type. The term ''criticality'' describes the impact of the total loss of a vessel or facility beyond the immediate local consequences and addresses regional or national impacts to human health, the economy and national security.

Finally, we scored the utility of TWIC in reducing vulnerability to terrorist attack for each vessel and facility type.

We used the AHP to combine these three factors and developed an overall risk ranking by vessel and facility type. AHP is a technique for decision making which uses a limited number of variables, each of which has a number of different attributes. This enables the combination of subjective and objective input from a group to produce consistent results.

Applying this technique, each of the three factors was weighted based on their importance to the policy decision process, and an analysis was conducted to check the consistency of the evaluation measures. At the end of this process, vessel and facility types with similar scores were combined into ''risk groups'' to determine TWIC verification and validation requirements.

In determining the cut offs between risk groups, risk rankings were graphed to identify any natural breaks that occurred in the data. For vessels, these breaks generally occurred where there was a change in the hazardous nature of the cargo or where the number of passengers carried aboard a vessel increased. The breaks were similar for facilities where these vessels called. These breaks were used in defining risk groups A, B, and C. These groups are spelled out in E. ''Facility and Vessel Risk Groups.''

We then turned to the Homeland Security Institute (HSI) to provide an independent peer review of our analysis.[3] Specifically, HSI is evaluating the validity of the risk assessment methodology and its appropriateness for the identified TWIC risk issues, the extent to which the conclusions follow from the analysis, and the overall strengths and weaknesses of the risk analysis. The main objective is to review how the MSRAM methodology has been applied to the development of the proposed TWIC reader requirements; the MSRAM methodology itself is not a part of the peer review. HSI's final report is expected this fall, and will be placed on the docket for this rulemaking, where indicated under **ADDRESSES**, as appropriate.

C. Requirement Options Considered

We considered three separate categories of TWIC verification that could, potentially, be checked at each entry: (1) Identity verification, (2) card authentication, and (3) card validity.

(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, this is done by matching the biometric template stored in the TWIC to the TWIC-holder's live sample biometric (*e.g.*, a fingerprint). However it can also be done to a less reliable degree by visually comparing the photo on the TWIC to the TWIC-holder or by requiring the TWIC-holder to place their card into a contact smart card reader and then entering his/her 6-digit Personal Identity Number (PIN), selected by the TWIC-holder at card issuance.

In some instances, a biometric match will not be possible. A small number of TWICs will be issued that contain either poor quality fingerprint templates, mostly due to badly damaged fingers, or no fingerprint minutiae in the case of amputations. In these cases, the reader will display a prompt indicating that this TWIC holder will require exception handling. We expect that the facility or vessel owner or operator will describe the exception process to be used in these cases in their security plan. The exception processes may include visual inspection of the TWIC including visual comparison of the photo printed on the card to the presented; visual comparison of the digital photo stored on the TWIC to the presenter by using a portable

[2] The ranking from each factor, as well as the overall rankings, are SSI per 49 CFR 1520.5(b)(5) and (b)(12). In accordance with 49 CFR 1520.9, SSI may only be released to covered persons with a need to know the information.

[3] The Homeland Security Institute (HSI) is a Studies and Analysis Federally Funded Research and Development Center established pursuant to section 312 of the Homeland Security Act of 2002 (6 U.S.C. 192). HSI delivers independent and objective analyses and advises in core areas important to its sponsor in support of policy development, decision-making, analysis of alternative approaches, and evaluation of new ideas on issues of significance.

reader with a contact interface and releasing the photo to the reader screen by entering the six-digit PIN; or an alternative process proposed by the owner or operator and approved by the Coast Guard.

Biometrics, other than the fingerprint templates stored in the Integrated Circuit Chip of the TWIC, may be used to biometrically verify the identity of individuals being granted unescorted access to secure areas of MTSA regulated facilities and vessels provided that a ''chain-of-trust'' is maintained to link the individual, their TWIC, and the alternative biometric. The process for maintaining these links would need to be described in an FSP or VSP, approved by the Coast Guard. In addition to linking the alternate biometric to the individual and heir TWIC, the process would need to include ascertaining the validity of the individual's TWIC.

Before obtaining an alternate biometric the TWIC holder must first be linked to their credential by matching the holder's fingerprint to the fingerprint template on the TWIC using a reader capable of reading and matching the TWIC biometric. During this process, the validity of the TWIC would also need to be ascertained. If the fingerprint template match is successful and the TWIC is valid the credential would, in most cases, be registered with the personnel access control system (PACS). While the TWIC holder is present, the alternate biometric would be captured and linked to the TWIC, thus establishing a ''chain-of-trust'' between the individual, their TWIC, and the alternate biometric. Variations on the usual process of registering the TWIC and alternate biometrics in a PACS, such as storing the alternate biometric on a separately issued card, or storing the alternate biometric on a local reader, may be proposed as part of the FSP or VSP. However, in all cases the linkage between the individual, the TWIC, and the alternate biometric would need to be proven and approved by the Coast Guard.

(2) Card authentication ensures that the card being used is an authentic TWIC, i.e., not a counterfeit. As designed, the primary method of card authentication involves engaging the TWIC with a reader to perform a CHALLENGE/RESPONSE protocol using the Card Authentication Certificate and the associated card authentication private key resident on the TWIC.[4] The card can also be visually inspected for various security features that are embedded into the front and back of the card, although this is a less reliable form of card authentication.

(3) Card validity involves the determination that a TWIC is still valid, i.e., that it has not expired; been reported as lost, stolen, or damaged; or been revoked for cause by TSA. A TWIC that is invalid is placed on the ''hotlist,'' which is updated daily.[5] As designed, checking for card validity is accomplished by comparing the expiration date of the TWIC to the current date and additionally comparing the card's internal Federal Agency Smart Card—Number (FASC–N), retrievable from several locations within the TWIC, to the hotlist FASC–Ns that TSA makes available to owners and operators.

An alternative method for checking card validity is to use a Certificate Revocation List (CRL). The link to the CRL is embedded in the Issuer Signing Certificate present on every card.[6] Each entry of the CRL is comprised of the certificate number and its date of revocation. Note there are four certificates for every TWIC Card (Card Authentication Certificate, Digital Signature Certificate, Key Management Certificate, and Personal Identity Verification (PIV) Authentication Certificate). The CRL is updated daily. Both of these processes (hotlist or CRL check) require a card/reader interface. A partial card validity check can be accomplished by reviewing the expiration date on the face of the TWIC, but such a check would not capture information relating to cardholders who TSA determines pose a security threat and/or hold revoked TWICs.

We anticipate that the Hotlist match (or the CRL match) can be done in one of two ways: Electronically (either in real time or by downloading the Hotlist into the reader or a separate access control system), or by printing out the Hotlist and manually entering it into a separate access control system.

The TWIC 1 NPRM discussed the potential for a process called ''privilege granting,'' in which an owner or operator could contact TSA and register those persons granted unescorted access privileges at the vessel or facility. Owners or operators would provide TSA with the FASC–Ns for every person who was being considered for unescorted access privileges. TSA would then contact the owner or operator directly if any of those FASC–Ns were placed on the Hotlist. This option requires access to a TWIC reader in order to discern the FASC–Ns associated with the individuals given unescorted access. This capability was tested during TSA's TWIC prototype but is not part of the current TWIC system. We would like to hear comments on whether such an option would be preferred, and if so, whether owners and operators would be willing to pay a fee for the option of using privilege granting (instead of downloading the Hotlist at regular intervals). If users would be willing to pay a fee, we also request a range of what would be appropriate (e.g., one time fee to use the system, annual fees, or a combination of both, plus limits on what fees owners and operators would be willing to pay).

D. Reader Requirements

When we considered electronic reader requirements for facilities and vessels, we began with a baseline approach that all three categories of TWIC verification—identity verification, card authentication, and card validity—in its most reliable and complete form should be required of all risk groups.

TWIC provides a universally recognized, tamper-resistant credential backed up by a TSA security threat assessment that, when used as an access control tool, reduces the risk of a transportation security incident at vessels and maritime facilities. TWIC is a dual interface smart card which was developed using national and international standards to ensure security, interoperability and performance. The card has physical and logical security features which, when used properly, can provide a secure method of determining, with a high level of assurance, that the TWIC-holder is the same individual to whom the TWIC was issued, and that they do not present a security threat.

The benefit of using existing industry recognized standards in developing the TWIC is the flexibility of use the card provides. It can be integrated into existing access control systems by using the TWIC as a secure means of

[4] The TWIC reader will read the Card Authentication Certificate from the TWIC card and then send a challenge 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 Card Authentication Certificate to verify the signature of the random data block is valid. If the signature is valid the TWIC reader will trust the TWIC card submitted and will proceed to pulling the Federal Agency Smart Credential—Number (FASC–N) and other information from the card for further processing. The Card Authentication Certificate contains the FASC–N and a certificate expiration date harmonized to the TWIC card expiration date. This minimizes the need for the TWIC reader to pull more information from the card (unless required for additional checking).

[5] The hotlist is online at: *https://twicprogram.tsa.dhs.gov/TWICWebApp/SDownloadHotlist.do.*

[6] The CRL is located at *http://twic-crl.orc.com/CRLs/TWICCA1.crl.*

authenticating an individual when first registering an individual into an existing access control system. Alternatively, either the contact or contactless interface can be used with existing smart card readers to authenticate the individual and the credential when making access control decisions, by securely accessing and using the data stored on the TWIC.

A design principle of the TWIC system is to establish and maintain a chain of trust. A chain of trust is a security architecture that ensures that a uniform level of security and integrity is applied to the components or agents where information is stored or passes through. TWIC accomplishes this by the use of secure communication between components of the TWIC system, identity verification and authentication issuance requirements, and centralized personalization.

The following tables briefly summarize the requirements the Coast Guard is considering for each risk group. It indicates what would need to occur, at each MARSEC Level, to complete identity verification, card authentication, and a card validity check.

TABLE OF POTENTIAL READER REQUIREMENTS

	MARSEC Level 1	MARSEC Level 2	MARSEC Level 3
Risk Group A, Bulk CDCs, >1,000 passengers	IDENTITY VERIFICATION: Biometric match of fingerprint to template stored in TWIC at each entry. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist weekly.	IDENTITY VERIFICATION: Biometric match of fingerprint to template stored in TWIC at each entry. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist daily.	IDENTITY VERIFICATION: Biometric match of fingerprint to template stored in TWIC at each entry. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist daily.
Risk Group B, HAZ MAT, Crude Oil, 500–1,000 passengers.	IDENTITY VERIFICATION: Random biometric match of fingerprint to template stored in TWIC, at least one day a month; all other times as visual identity badge. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist weekly.	IDENTITY VERIFICATION: Biometric match of fingerprint to template stored in TWIC at each entry. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist daily.	IDENTITY VERIFICATION: Biometric match of fingerprint to template stored in TWIC at each entry. CARD AUTHENTICATION: Electronic communication to achieve a successful CHALLENGE/RESPONSE result at each entry. CARD VALIDITY CHECK: Compare FASC–N against Hotlist at each entry; update Hotlist daily.
Risk Group C, Non-HAZ MAT, <500 passengers MODU OSV.	IDENTITY VERIFICATION: Visual identity badge at each entry. CARD AUTHENTICATION: Check security features on card at each entry and electronic verification during annual inspections and random spot checks. CARD VALIDITY CHECK: Check expiration date at each entry; CG perform spot checks.	IDENTITY VERIFICATION: Visual identity badge at each entry. CARD AUTHENTICATION: Check security features on card at each entry and electronic verification during annual inspections and random spot checks. CARD VALIDITY CHECK: Check expiration date each entry; CG perform spot checks.	IDENTITY VERIFICATION: Visual identity badge at each entry. CARD AUTHENTICATION: Check security features on card at each entry and electronic verification during annual inspections and random spot checks. CARD VALIDITY CHECK: Check expiration date at each entry; CG perform spot checks.

Risk Group A

To provide the maximum security benefit, we determined that those assets presenting the highest risk should be required to implement the most protective measures. Thus, we are considering requiring facilities and vessels that fall into risk group A to either match the TWIC-holder's biometric (fingerprint) to the template stored in the card or to match the TWIC-holder's biometric to one held in the owner/operator's own access control system. This match will need to occur at each entry. For the latter option, the owner or operator may choose to apply a different biometric than the fingerprint, such as an iris scan or hand geometry, stored in the local access control system and matched to the individual seeking access. Also, for the latter option, the owner/operator's system must be linked to the TWIC in such a manner that the access control system forbids access to someone who does not have a valid TWIC, or to someone other than to whom the TWIC has been issued. This means that the TWIC will need to be read and the stored biometric identifier matched against the TWIC-holder's fingerprint at least once, when the individual is entered into the local access control system.

We are re-considering whether to require a TWIC-holder to verify his/her PIN as a part of the identity verification process. This added element, making the TWIC-holder provide ''something he/she knows,'' would complete three-factor authentication: (1) Something the person has—a TWIC credential; (2)

Something the person knows—a PIN, stored securely on * * * the credential; and (3) Something the person is—biometric. PIN verification would require the TWIC to be inserted into a card reader, as the PIN only operates in the contact-chip mode. Comments received on the TWIC 1 NPRM made it clear that requiring insertion of a TWIC into an open-slot card reader was not favored among the maritime community. This was echoed in the recommendations made by NMSAC in its recommendations for specifications for a contactless TWIC. There were concerns over whether the readers would be able to withstand harsh environmental and operational conditions and how long they would last if they were operated continually in the maritime environment. Industry partners also voiced concerns over whether maritime workers would be able to remember a PIN, especially if a PIN was only required at higher MARSEC Levels, and over the operational delays that may be caused by requirements for TWIC-holders to pass through access control points, insert the card, enter a PIN (which could take several tries), and then remove the card. After considering these comments, the relative risk presented by the vessels and facilities, and the security already being provided through the remaining requirements, we have tentatively determined that a requirement for use of the PIN would have a negative impact on large scale throughput during access control evolutions. As a result, we have not included a requirement for regular use of the PIN at any MARSEC Level for any risk group in this ANPRM. We would like public comments on this decision and whether the Coast Guard should reconsider using PIN requirements. We note, however, that PINs may be required by owners and operators who wish to implement an additional level of security or during the spot checks and annual inspections conducted by the Coast Guard.

We are also considering a proposal that vessels and facilities in the highest risk group (risk group A) authenticate the card electronically with a card reader at each entry. Again, for vessels and facilities opting to integrate TWIC into existing local access control systems, this will need to be done before the individual's information is added into the local access control system, and before unescorted access is first granted to the individual. For other vessels and facilities, this function can be done by TWIC readers at the same time that the biometric match is being made. Adding this requirement would add a negligible time to the transaction between the TWIC-holder and the card reader, as the readers will be able to perform this function as the individual is presenting his or her finger for matching against the template stored on the TWIC.

Finally, vessels and facilities in risk group A would verify the validity of the TWIC at each entry using information that is no more than seven (7) days old, when at MARSEC Level 1. This means that on a weekly basis, the Hotlist or CRL will need to be downloaded into the reader(s) used at the vessel or facility's access control point(s) or into the local access control system used by the vessel or facility. This frequency will jump to daily (i.e., the Hotlist or CRL will need to be downloaded daily) at MARSEC Levels 2 and 3. We request comments, particularly from vessels and facility owners and operators in risk grouping A, as to these processes.

Risk Group B

Vessels and facilities in risk group B would, under a final rule based on this model, be required to complete the identity verification by using the TWIC as a visual identity badge (''flash pass'') at each entry. On a random basis, but at least one day a month, at MARSEC Level 1, they would also be required to match the biometric stored on the card in order to conduct more complete identity verification.

Vessels and facilities in risk group B would need to perform card authentication by electronically reading all the cards at MARSEC Level 1 at each entry, even when the biometric match is not being implemented. While these checks require the use of an electronic reader, they may be done using the contactless smart card interface, and would not require that the individual TWIC-holder present his or her fingerprint for matching against the template. The validity of the TWICs must be checked at each entry, using TSA's Hotlist or CRL. At MARSEC Level 1, this would be done using information that is no more than seven (7) days old. At MARSEC Levels 2 and 3, the information would be downloaded daily. We seek comments on this process and its application to vessels and facilities in risk group B.

Risk Group C

Facilities and vessels in the lowest risk group, risk group C, would not be required to match the biometric stored on the card in order to complete the identity verification at any MARSEC Level. Instead, they would only be required to use the TWIC as a visual identity badge in the manner currently required by the TWIC 1 FR. This provides identity verification with a lower level of reliance than a biometric match would, however, we have determined at this time, and subject to public comment, that in this lower risk group matching the biometric frequently is not necessary. Given the type of commodities and small number of passengers typical of this risk group, it is likely these vessels and facilities are a less attractive target for individuals who wish to do harm, though still holding the potential of being involved in a TSI. As a result, we have determined that the frequent matching of a biometric would not be practical. In addition, identity verification using TWIC as a visual identity badge would more closely align with other less stringent security provisions implemented at these lower risk vessels and facilities.

Card authentication for this group (risk group C), would require only verification of the various security features on the front and back of the card. Under this process, vessels and facilities in this risk group would continue to use the TWIC in the manner required by the TWIC 1 FR. Finally, for the card validity check, we would require only that the expiration date be checked. Thus, vessels and facilities in risk group C will be able to fulfill their TWIC obligations without having to buy or have access to a card reader.

This does not mean that individuals who hold TWICs and work exclusively at vessels or facilities falling into risk group C will never need to present their TWICs for a biometric match or more secure card authentication check. The Coast Guard will continue to check and verify TWICs, using handheld readers, during annual inspections and during unannounced spot checks aboard vessels and facilities within all three risk groups. These checks will include identity verification using the fingerprint template stored in the TWIC, card authentication, and card validity checks using the current TSA Hotlist or CRL. Additionally, vessels and facilities may choose to electronically authenticate the card with a card reader.

TSA would be able, through use of information collected during enrollment for the TWIC, to contact employers or the Coast Guard if an imminent threat, resulting in an immediate revocation of a TWIC, is identified during the perpetual vetting of TWIC holders. At MARSEC Levels 2 or 3, the Coast Guard spot checks and the percentage of TWICs verified at each annual inspection would increase.

The Coast Guard seeks public comment of these processes, and specifically as to the everyday

operational impacts related to the process and whether they will maintain appropriate security levels while permitting the efficient and effective continuation of industry operations.

E. Facility and Vessel Risk Groups

The following are suggested risk groups for vessels that are subject to 33 CFR part 104:

Risk Group A

(1) Vessels that carry Certain Dangerous Cargoes (CDC) in bulk;
(2) Vessels certificated to carry more than 1,000 passengers; and
(3) Towing vessels engaged in towing a barge or barges subject to paragraphs (1) or (2).

Risk Group B

(1) Vessels that carry hazardous materials other than CDC in bulk;
(2) Vessels subject to 46 CFR Chapter I, Subchapter D, that carry any flammable or combustible liquid cargoes or residues [7];
(3) Vessels certificated to carry 500 to 1,000 passengers; and
(4) Towing vessels engaged in towing a barge or barges subject to paragraphs (1), (2), or (3).

Risk Group C

(1) Vessels carrying non-hazardous cargoes that are required to have a vessel security plan;
(2) Vessels certificated to carry less than 500 passengers;
(3) Towing vessels engaged in towing a barge subject to paragraphs (1) or (2);
(4) Mobile Offshore Drilling Units (MODU); and
(5) Offshore Supply Vessels (OSVs) subject to 46 CFR chapter I, subchapters L or I.

The following is suggested risk groups for facilities that are subject to 33 CFR part 105:

Risk Group A

(1) Facilities that handle CDC in bulk;
(2) Facilities that receive vessels certificated to carry more than 1,000 passengers; and
(3) Barge fleeting facilities that receive barges carrying CDC in bulk.

Risk Group B

(1) Facilities that receive vessels that carry hazardous materials other than CDC in bulk;
(2) Facilities that receive vessels subject to 46 CFR Chapter I, Subchapter D, that carry any flammable or combustible liquid cargoes or residues;
(3) Facilities that receive vessels certificated to carry 500 to 1,000 passengers; and
(4) Facilities that receive towing vessels engaged in towing a barge or barges carrying hazardous materials other than CDC in bulk, crude oil, or certificated to carry 500 to 1,000 passengers.

Risk Group C

(1) MTSA-regulated facilities that receive vessels carrying non-hazardous cargoes that are required to have a vessel security plan;
(2) Facilities that receive towing vessels engaged in towing a barge carrying non-hazardous cargoes;
(3) Facilities that receive vessels certificated to carry less than 500 passengers.

All OCS facilities subject to 33 CFR part 106 would fall into risk group B.

We considered the possibility that vessels may move from one risk group to another, based on the cargo they are carrying or handling at any given time. We expect that owners and operators of vessels that expect to be in this situation (of moving between risk groups) will explain, in their amended security plans, how they will move between the requirements of the higher and lower risk groups, with particular attention to the security measures to be taken when moving from a lower risk group to a higher risk group and seek comments regarding this requirement and the potential timing and processes for carrying out these amendments.

We have also considered the possibility that facilities could be permitted to move between risk groups based on vessel interface or cargo operations. We are specifically requesting comment and suggestions on how to apply this flexibility as it pertains to potential electronic reader requirements while ensuring an equivalent level of security and consistency across multiple COTP Zones to the maximum extent possible.

F. Recurring Unescorted Access

In the TWIC 1 NPRM, we introduced the concept of recurring unescorted access for vessels to allow an individual to enter on a continual basis, without repeating the identity verification requirement at each entry. 71 FR 29410. This concept allowed flexibility for an individual to acquire unescorted access to secure areas on a continual or ongoing basis, without having to fulfill the TWIC access control requirement at every entry. In that NPRM, we noted that an owner or operator's decision to grant recurring unescorted access should be based on two considerations: (1) The relationship of the individual to the vessel, or how well ''known'' he or she is; and (2) the individual's need to have frequent and unimpeded access to the vessel. In developing this ANPRM, we determined that both vessels and facilities, at each risk group, should have the option of using recurring unescorted access for up to 14 persons per vessel or facility, if that provision is included in their amended security plan and approved by the Coast Guard. In order to take advantage of recurring unescorted access, the owner or operator of the vessel or facility would need to perform a biometric match of the individual against his or her TWIC (identity verification), either at hiring or upon the effective date of a final rule, whichever occurs later. This biometric match would need to include a verification of the FASC–N and the TWIC Card Authentication Certificate (card authentication), as well as a verification of the validity of the TWIC (card validity check). Once this check is done, the TWIC could be used as a visual identity badge at a frequency to be approved by the Coast Guard in the amended security plan, so long as the validity of the TWIC is verified periodically, using the Hotlist or CRL. For vessels and facilities in risk groups A and B, these periodic checks of validity would need to occur on a weekly basis at MARSEC Level 1, and on a daily basis at MARSEC Levels 2 and 3. For those vessels in risk group C, these checks would need to occur on a monthly basis at MARSEC Level 1, and on a weekly basis at MARSEC Levels 2 and 3. In each case, the validity would need to be checked using information that is no more than 24 hours old.

As a result, vessels in any risk group with a crew of 14 or less would not need to carry a reader on their vessel to provide access control over his or her own crew. The owner or operator would need access to a reader to perform the initial identity verification and card authentication, and would likely need some specialized software on a computer to complete the card validity checks, but these checks could be done at a shore side location, such as at the company's office. This would allow owners and operators of more than one vessel to use the same reader for an entire fleet. It also enables the owner or operator to pursue an agreement with a facility or other company to borrow or otherwise have access to their reader to perform the initial check, create a file with the FASC–Ns and names of the employees granted recurring unescorted access, and then use a software program

[7] The intent as used here is to capture those tank vessels that are carrying the high flash point petroleums, like crude oil, that aren't hazardous materials, whether inland, coastal, or seagoing.

to compare this list to the TSA Hotlist or CRL on the required periodic basis.

We used the recommendation from the Towing Safety Advisory Committee (TSAC) which recommended a crew size cut off of 14 for determining when to require a reader on board a vessel, as required by the SAFE Port Act to develop a cut off for recurring unescorted access. This was done because the rationale for allowing recurring unescorted access—i.e., that these vessels have a reduced vulnerability because the individuals are all ''known'' to one another—is the same rationale used by TSAC to justify their crew size cut off recommendation. The number was developed by taking into account the fact that for a small vessel, such as a towing vessel or offshore supply vessel, the crew would typically include up to one Master, one Chief Engineer, and three four-person crews who rotate through watch shifts. This number would also include a large percentage of deep draft vessels. We then carried the number over to facilities, as it is reasonable to assume that 14 persons could be ''known'' by a facility owner or operator as well.

While the recurring unescorted access provision does not go so far as to set a specific crew size below which a reader would not be required on a vessel, we believe this provision, in conjunction with the no reader requirement for risk group C, meets the intent of the SAFE Port Act. Namely, it provides relief for owners and operators of small and many large vessels, where it is unlikely that someone unknown to the crew could acquire any type of access to the vessel without raising suspicion. Additionally, while the recurring unescorted access process would call for the use of electronic card readers to gain access to certain vessels, we would not require that they be carried on board any vessel. If the owner or operator of a vessel can demonstrate in their vessel security plan that they will be able to meet the reader requirements via use of a reader at a dedicated facility, by using a reader that stays ashore with the company, or by agreements established between vessels and facilities (such those captured in a Declaration of Security) then the recurring unescorted access provisions could be met without requiring installation or implementation of a reader on a gangway or at any other place on the vessel.

G. Additional Topics and Requirements

Reader Approval—TWIC readers, incorporated into MTSA regulated vessel and facility PACS, will need to follow the standard/specification that will be developed from the results of the TWIC reader pilot program, and published by the Government. An independent lab that tests for compliance to the standard will be used by reader manufacturers. These test results will be listed by the Government on the DHS Responder Knowledge Base (RKB), which provides an on-line source of information on products, equipment, and other information. The RKB Web site may be viewed at: *http://www.rkb.us.*

Reader Calibration and Compliance—we are considering alternatives for how we can check for compliance with regard to the readers themselves. We would like to ensure, that once readers are installed, they are maintained in proper working order. The existing provisions in 33 CFR 104.235, 104.2260, 105.225, 105.250, 106.230, and 106.255 would require that the readers be inspected, tested, calibrated, and maintained in accordance with the manufacturer's recommendations, and that records of those actions be maintained as well. We seek comment on whether TWIC readers should also be the subject to Coast Guard inspections, or require some type of third party audit.

Security Plan amendment—we are considering a requirement for all owners and operators to amend their security plans to include TWIC requirements. We intend, at this time, to require the amendment within six months of promulgation of a final rule. However, we will re-evaluate this deadline as we get closer to issuing a final rule. We are also considering the staggering of deadlines in order to spread out expiration dates for security plans in the future. We seek public comment on how long owners and operators should have to amend security plans to incorporate TWIC reader requirements. This amendment would need to detail how the owner or operator would implement the TWIC verification requirements, including those promulgated in the TWIC 1 FR (if not already incorporated into their security plans), and electronic reader requirements if applicable. For instance, if the owner or operator will use recurring unescorted access, the amendment would need to explain when and where the initial check of the TWIC will occur, as well as how the periodic card validity check will be accomplished. The amendment would also need to explain how the owner or operator would address identity verification, TWIC authentication, and the TWIC validity check for individuals who are not granted recurring unescorted access (i.e., how they would check TWICs according to the relevant requirements if an individual seeks unescorted access, or how escorting would be accomplished).

Additional security plan provisions that we are considering include requiring the owner or operator to discuss how they will handle those persons whose TWIC indicate they have poor quality or no fingerprints, as well as those persons that are unable to match their live fingerprint to the template stored on their TWIC. We are also considering adding a requirement that those owners and operators using a separate physical access system explain how they are protecting personal identity information.

Requests for waivers, alternatives, and equivalents would need to comply with existing regulatory requirements found in 33 CFR 101.120, 101.130, 104.130, 104.135, 105.130, 105.135, 106.125 and 106.130.

We would not amend the section on Alternative Security Programs (ASPs), 33 CFR 101.120. Rather, we expect that, should this process be promulgated in a final rule, the Coast Guard will exercise its existing authority, found in § 101.120(d)(1)(ii), to require those organizations that have approved ASPs to amend them to incorporate the TWIC requirements. We will give each organization the same amount of time that owners and operators have to complete this amendment, but seek comment on whether a shorter or longer period would be more appropriate. For those organizations whose current ASPs cover vessels or facilities that would fall into more than one risk group, we would expect that the amended ASP address each relevant risk group.

Recordkeeping—The electronic readers that will be available for owners and operators to purchase in order to meet the requirements included in this proposal should be able to keep track of the names, FASC–Ns, dates, and times of those persons passing through the reader. Having records of those persons who were granted unescorted access, may prove beneficial in law enforcement situations. For this reason, we are considering requiring that facility and vessel owners who are required to utilize readers (those in risk groups A and B) also keep records of the persons who have been granted unescorted access (those whose TWICs have been read by a card reader) for a period of two years. We are not considering requiring that owners and operators need to know who is on their vessel or facility at all times and believe that type of requirement would be burdensome compared to the security benefit that it would provide. This would remove the requirement that individuals have their TWICs

electronically read when leaving the facility or vessel.

We are also considering that owners and operators opting to use recurring unescorted access keep records of those persons to whom recurring unescorted access has been granted. We would not be prescribing the format for these records, only that they include the name of individuals granted recurring unescorted access and be kept for two years and made available to the Coast Guard upon inspection or request. These records must allow the Coast Guard to identify the 14 (or fewer) individuals who are using the recurring unescorted access privilege at the time they inspect or request the record.

We are also considering a provision that all owners and operators maintain a record to demonstrate that they have completed the card validity check (Hotlist or CRL check), if required.

Additional persons required to obtain TWICs—MTSA contained additional categories of individuals who must hold a TWIC that were not explicitly identified in the TWIC 1 NPRM or TWIC 1 FR. These include all vessel pilots and all persons engaged on a towing vessel that pushes, pulls, or hauls alongside a tank vessel. 46 U.S.C. 70105(b). We believe that the majority of these individuals were already captured in the TWIC 1 FR requirement for all persons requiring unescorted access to secure areas; however there may be some vessel pilots that do not hold Federal licenses, and there may be some persons who are not credentialed mariners who are engaged on a towing vessel that is not otherwise regulated by 33 CFR part 104. Thus, we are considering including these populations in the TWIC requirement when we issue an NPRM, in order to comply with the congressional mandate found in 46 U.S.C. 70105(b).

V. Advisory Committee Input

The Coast Guard has a long tradition of consulting with its advisory committees before taking regulatory action. We acknowledge the benefit of consulting with our advisory committees, and before issuing this ANPRM we sent a task statement to the Merchant Marine Personnel Advisory Committee (MERPAC), TSAC, and NMSAC, asking eighteen questions related to requirements for TWIC readers. This task statement, as well as each committee's formal responses and recommendations, may be found in the docket for this ANPRM where listed under the **ADDRESSES** section above. As discussed above, we accepted and incorporated a number of the advisory committee recommendations into this ANPRM. We greatly appreciate advisory committee input into this program and plan to continue to seek advisory committee input throughout the remainder of the TWIC regulatory process.

VI. Discussion of Pilot Program

In accordance with the SAFE Port Act, DHS, through the USCG and TSA, developed a pilot program to ''test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system.'' 46 U.S.C. 70105(k)(1)(A). The SAFE Port Act requires the pilot program to be conducted in a minimum of five geographically distinct locations. The selected sites include the ports of Los Angeles and Long Beach, California; the ports of New York and New Jersey, (New York, Elizabeth, and Newark); the port of Brownsville, Texas; an Inland Rivers tugboat operator in Vicksburg, Mississippi; the Staten Island Ferry in New York, and a small passenger vessel operator in Annapolis, Maryland. Other locations are also under consideration, specifically a cold weather facility in the Great Lakes region. The goal of the pilot program site selection is to engage a wide range of vessel and facility types in a variety of operational environments and geographic areas. During the reader pilot program, TSA strongly advocates, but does not mandate, that port security directors consider FIPS 201 authentication readers to accommodate future FIPS 201 interoperable cards.

The TWIC pilot program will conduct tests of contactless biometric readers, as well as the credential authentication and validation process to evaluate the previously published reader specification. 72 FR 53784. TSA and USCG worked with the maritime and smart card industries through NMSAC to specify contactless technology for TWIC readers that will minimize the impact to the flow of commerce (*e.g.*, slower throughput at gates, potential lower availability of workers) while still enabling the use of biometrics to verify identity and while protecting personal information in the card from unauthorized disclosure. The following should not be considered an all-inclusive list; rather, this information is intended to offer insight regarding the purpose and goals of the TWIC pilot program to greater inform your comments to this ANPRM and provide information as to the overall progress of the TWIC program.

TSA has developed a Test and Evaluation Master Plan (TEMP) to provide a plan to acquire and evaluate the test data needed to support the final reader rule. The TEMP addresses the impact of requiring the use of the Contactless Biometric Card Reader to biometrically verify identity, card authenticity and validity, and establishes a plan for an Integrated Test and Evaluation Program (ITEP) for the card reader. The ITEP is designed to provide accurate and timely information necessary to evaluate the economic impact of a nationwide deployment of the card reader(s), and to test the capability of card reader(s) to support the enhanced security of the Nation's maritime transportation systems through the development and issuance of enhanced rules and specifications. The ITEP is comprised of three principle activities including:

(1) Initial Technical Test (ITT),

(2) Early Operational Assessment (EOA), and

(3) System Test and Evaluation (ST&E).

All testing is designed to build upon preceding testing and assessments to ensure all technical and operational aspects of the card reader are evaluated while minimizing testing duplication.

The ITT is focused on providing information to determine if select card readers meet specification parameters, including environmental requirements, to ensure that the card readers will correctly perform the biometric match and operate in the maritime operational environment during ST&E.

The EOA is focused to obtain essential data to support rulemaking, assess card reader suitability and effectiveness, and support refinement of the card reader specification.

The ST&E is a comprehensive technical and operational testing of the card reader system to provide the information required to finalize reader regulatory requirements and support future card reader acquisitions by the stakeholders.

Reader conformance testing is predicated upon a test protocol verified by the National Institute of Standards and Technology. Conformance testing will be conducted in accordance with the test protocol at an independent laboratory. This includes TWIC contactless reader interface testing.

Upon successful completion of the ST&E conformance testing, card readers and/or portable card readers are installed and tested at selected operational sites and vessels. The operational testing will proceed with the system operating at the site or vessel. System testing then continues until the data to support the decision for declaration of operational effectiveness and supportability is acquired.

As required by the SAFE Port Act, the pilot program's results should validate the TWIC and TWIC reader's impact on the flow of commerce, the ability for vessels and facilities to comply with the regulations, the applicability of the TWIC reader requirements, and their ability to improve security, and economic and environmental impacts.

VII. Regulatory Analyses

Before developing an NPRM, we will consider a number of statutes and executive orders related to rulemaking, including Executive Orders 12866 and 13132 (Regulatory Planning and Review and Federalism, respectively), the Regulatory Flexibility Act (5 U.S.C. 601–612), the Paperwork Reduction Act (44 U.S.C. 3501–3520), and the National Environmental Policy Act of 1969 (42 U.S.C. 4321–4370f). If you have any information or comments that you feel would be helpful to us as we complete these required analyses, please submit it to the docket during the comment period for this ANPRM. Draft analyses will be included as part of an NPRM, and will be made public for comment before the issuance of a final rule, as required by the Administrative Procedure Act (5 U.S.C. 553).

Dated: January 16, 2009.

Brian M. Salerno,

Rear Admiral, U.S. Coast Guard, Assistant Commandant for Marine Safety, Security and Stewardship.

[FR Doc. E9–6852 Filed 3–26–09; 8:45 am]

BILLING CODE 4910–15–P

POSTAL REGULATORY COMMISSION

39 CFR Part 3007

[Docket No. RM2008–1; Order No. 194]

Treatment of Non-Public Materials Submitted by the Postal Service

AGENCY: Postal Regulatory Commission.

ACTION: Proposed rule.

SUMMARY: The Commission is proposing rules on the treatment of non-public material submitted by the Postal Service. Issuance of this proposal will allow interested parties to comment on the Commission's approach to implementing a new statutory requirement.

DATES: Initial comments due April 27, 2009; reply comments due May 11, 2009.

ADDRESSES: Submit comments electronically via the Commission's Filing Online system at *http://www.prc.gov*.

FOR FURTHER INFORMATION CONTACT: Stephen L. Sharfman, General Counsel, 202–789–6820 and *stephen.sharfman@prc.gov*.

SUPPLEMENTARY INFORMATION: *Regulatory History*, 73 FR 50532 (August 26, 2008).

I. Introduction

The Postal Regulatory Commission (Commission) proposes to implement 39 U.S.C. 504(g) by adopting regulations applicable to confidentiality of materials submitted by the Postal Service to the Commission. A Notice of Proposed Rulemaking to Establish a Procedure for According Appropriate Confidentiality, issued August 13, 2008 (Order No. 96), requested public comments and reply comments. Based on comments received in this docket (RM2008–1) in response to the Commission's initial notice, the Commission issues this Second Notice of Proposed Rulemaking to Establish a Procedure for According Appropriate Confidentiality.

39 U.S.C. 504(g)(3)(A) recognizes the need to balance the Postal Service's, its business partners', or its customers' legitimate expectations to keep commercially sensitive information confidential with the public's expectation for accountability and transparency of the business dealings of a governmental entity competing in commercial markets. The Postal Accountability and Enhancement Act (PAEA), Public Law 109–435, 120 Stat. 3218 (2006), relies on public transparency, in addition to regulation, to achieve its goal of Postal Service accountability. Therefore, as directed by the provisions of the PAEA and because the Commission considers it necessary and appropriate, the Commission proposes rules that could lead to public disclosure of materials that the Postal Service or a third party initially claims are non-public.

In developing proposed rules, the Commission takes very seriously its responsibility to achieve a fair balance between the commercial interests of the Postal Service and its partners or customers and the public interest in disclosure of information concerning a public entity that competes in commercial markets, as well as the need for discovery and access for any persons who wish to participate in Commission proceedings.

II. Statutory Standards for According Confidentiality to Postal Service Materials

The Postal Regulatory Commission is an independent establishment of the executive branch of the Government of the United States. *See* 39 U.S.C. 501. Therefore, the presumption is that its records are available for public review. 5 U.S.C. 552. However, 39 U.S.C. 504(g)(1) provides that the Postal Service may determine ''that any document or other matter it provides to the Postal Regulatory Commission'' is exempt from public disclosure under 39 U.S.C. 410(c) or 5 U.S.C. 552(b). The Postal Service must give reasons, in writing, for its claim. *See* 39 U.S.C. 504(g)(1).

Unless the Commission has established rules for determining the appropriate degree of protection of materials claimed to be non-public by the Postal Service, the Commission may not (1) ''use such information for purposes other than the purposes for which it is supplied;'' or (2) ''permit anyone who is not an officer or employee of the Commission to have access to any such information.'' *See* 39 U.S.C. 504(g)(2).

These proposed rules outline the procedure for the Commission's treatment of non-public materials. Under these proposed rules, when materials are filed along with an application for non-public treatment, the Commission will initially treat those materials as non-public. However, the proposed rules allow persons to challenge non-public status or request access to the materials. The Commission, following such a motion or of its own accord, may balance the relevant interests to determine if disclosure or access is warranted.

Under 39 U.S.C. 410(c), the Postal Service may claim as exempt from public disclosure the name and address of postal customers; certain commercial information, for example, trade secrets, and other information which would not be disclosed under good business practice; certain information related to the negotiation of collective bargaining agreements; information prepared for proceedings before the Commission or the Federal courts concerning postal rates, classes and services; reports and memoranda prepared by outside sources unless their disclosure would have been required if the Postal Service had prepared the reports or memoranda itself; and investigatory files compiled for law enforcement purposes, unless legally available to parties other than the Postal Service.

Under 5 U.S.C. 552(b), records that may be withheld from public disclosure include, but are not limited to, matters concerning only internal personnel matters of an agency; matters specifically exempted from public disclosure by statute; trade secrets and privileged or confidential commercial or financial information; non-public