Federal Register

Thursday,
January 25, 2007

Part II

Department of Homeland Security

Coast Guard

33 CFR Parts 1, 20 et al. and 46 CFR Parts 1, 4 et al.

Transportation Security Administration

49 CFR Parts 10, 12, and 15

Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Final Rule

Consolidation of Merchant Mariner Qualification Credentials; Proposed Rule

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 101, 103, 104, 105, 106, 125 and 46 CFR Parts 10, 12, 15
Transportation Security Administration
49 CFR Parts 1515, 1540, 1570, 1572
[Docket Nos. TSA–2006–24191; Coast Guard–2006–24196; TSA Amendment Nos. 1515–(New), 1540–8, 1570–2, 1572–7]

RIN 1652–AA41

Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License

AGENCY: Transportation Security Administration; United States Coast Guard, DHS.

ACTION: Final rule; request for comments.

SUMMARY: The Department of Homeland Security (DHS), through the Transportation Security Administration (TSA) and the United States Coast Guard (Coast Guard), issues this final rule to further secure our Nation's ports and modes of transportation. This rule implements the Maritime Transportation Security Act of 2002 and the Security and Accountability for Every Port Act of 2006. Those statutes establish requirements regarding the promulgation of regulations that require credentialed merchant mariners and workers with unescorted access to secure areas of vessels and facilities to undergo a security threat assessment and receive a biometric credential, known as a Transportation Worker Identification Credential (TWIC). After DHS publishes a notice announcing the compliance date for each Captain of the Port (COTP) zone, persons without TWICs will not be granted unescorted access to secure areas at affected maritime facilities. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners must possess a TWIC by September 25, 2008. This final rule will enhance the security of ports by requiring such security threat assessments of persons in secure areas and by improving access control measures to prevent those who may pose a security threat from gaining unescorted access to secure areas of ports.

With this final rule, the Coast Guard amends its regulations on vessel and facility security to require the use of the TWIC as an access control measure. The Coast Guard also amends its merchant mariner regulations to incorporate the requirement to obtain a TWIC. This final rule does not include the card reader requirements for owners and operators set forth in the Notice of Proposed Rulemaking (NPRM) issued in this matter on May 22, 2006. Such requirements will be addressed in a future rulemaking. Although the card reader requirements are not being implemented at this time, the Coast Guard will institute periodic unannounced checks to confirm the identity of the holder of the TWIC.

With this final rule, TSA applies its security threat assessment standards that currently apply to commercial drivers authorized to transport hazardous materials in commerce to merchant mariners and workers who require unescorted access to secure areas on vessels and at maritime facilities. This final rule amends TSA regulations in a number of ways. To minimize redundant background checks of workers, TSA amends the threat assessment standards to include a process by which TSA determines if a security threat assessment conducted by another governmental agency or by TSA for another program is comparable to the standards in this rule. TSA amends the qualification standards by changing the list of crimes that disqualify an individual from holding a TWIC or a hazardous materials endorsement.

TSA expands the appeal and waiver provisions to apply to TWIC applicants and air cargo employees who undergo a security threat assessment. These modifications include a process for the review of adverse waiver decisions and certain disqualification cases by an administrative law judge (ALJ). TSA also extends the time period in which applicants may apply for an appeal or waiver.

Finally, this rule establishes the user fee for the TWIC and invites comment on one component of the fee, the card replacement fee.

Under this rule, TSA will begin issuing first generation TWIC cards at initial port deployment locations. These TWIC cards will not initially support contactless biometric operations, but the TWIC cards will be functional with certain existing access control systems in use at ports today.

TSA and the Coast Guard have established a working group, comprised of members of the maritime and technology industries, through the National Maritime Security Advisory Committee (NMSAC), a federal advisory committee to the Coast Guard. This working group, in consultation with the National Institute for Standards and Technology (NIST), is tasked with recommending the contactless biometric software specification for TWIC cards.

TSA will publish a notice detailing the draft contactless biometric software specification for TWIC cards no later than the date by which it publishes the final TWIC fee as required by this Rule. Currently those notices are expected to be published in February 2007. TSA will subsequently publish a final specification for TWIC contactless biometric software functionality and the associated specifications for TWIC card readers. TSA plans also to write electronically the contactless biometric software application to all issued TWIC cards after publication of this specification. After initial field testing, this additional contactless biometric function will be included with all TWIC cards produced after publication of the contactless biometric software specification.

Although this rule goes into effect on March 26, 2007, the requirements to hold a TWIC, and to restrict access to secure areas of a facility or OCS facility, will be effective only after the regulated party is notified by DHS. These notifications will be published in the **Federal Register** and will require compliance on a COTP by COTP basis. Those seeking unescorted access to secure areas aboard affected vessels, and all Coast Guard credentialed merchant mariners must possess a TWIC by September 25, 2008.

DATES: *Effective Date:* This rule is effective March 26, 2007.

Comment Date: Comments with respect to the Card Replacement Fee must be submitted by February 26, 2007.

ADDRESSES: Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of dockets TSA–2006–24191 and Coast Guard–2006–24196 and are available for inspection or copying at the Docket Management Facility, U.S. Department of Transportation, room PL–401, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at *http://dms.dot.gov.*

You may submit comments identified by docket number TSA–2006–24191 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

(1) *Web Site: http://dms.dot.gov.*

(2) *Mail:* Docket Management Facility, U.S. Department of Transportation, 400

Seventh Street SW., Room PL–401, Washington, DC 20590–0001.

(3) *Fax:* 202–493–2251.

(4) *Delivery:* Room PL–401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

(5) *Federal eRulemaking Portal: http://www.regulations.gov.*

See **SUPPLEMENTARY INFORMATION** for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: For questions related to TSA's standards: Greg Fisher, Transportation Security Administration, TSA–19, 601 South 12th Street, Arlington, VA 22202–4220, TWIC Program, (571) 227–4545; e-mail: *credentialing@dhs.gov.*

For legal questions: Christine Beyer, TSA–2, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202–4220; telephone (571) 227–2657; facsimile (571) 227–1380; e-mail *Christine.Beyer@dhs.gov.*

For questions concerning the Coast Guard provisions of the TWIC rule: LCDR Jonathan Maiorine, Commandant (G–PCP–2), United States Coast Guard, 2100 Second Street, SW., Washington, DC 20593; telephone 1–877–687–2243.

For questions concerning viewing or submitting material to the docket: Renee V. Wright, Program Manager, Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street, SW., Washington, DC 20590–0001; telephone (202) 493–0402.

SUPPLEMENTARY INFORMATION:

Comments Invited

TSA invites comment on one provision of the rule, the Card Replacement Fee, as discussed in section I under Fees and section VI of this preamble. See **ADDRESSES** above for information on where to submit comments. With each comment, please include your name and address, identify the docket number at the beginning of your comments, and give the reason for each comment. Please explain the reason for any recommended change and include supporting data. You may submit comments and material electronically, in person, by mail, or fax as provided under **ADDRESSES,** but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you want TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

TSA will file in the public docket all comments received by TSA, except for comments containing confidential information and sensitive security information (SSI)[1], TSA will consider all comments received on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or 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 SSI 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 address listed in the **FOR FURTHER INFORMATION CONTACT** section. Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's (DHS's) FOIA regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to 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 the applicable Privacy Act Statement published in the **Federal Register** on April 11, 2000 (65 FR 19477), or you may visit *http://dms.dot.gov.*

You may review the comments in the public docket by visiting the Dockets Office between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The Dockets Office is located on the plaza level of the Nassif Building at the Department of Transportation address, previously provided under **ADDRESSES.** Also, you may review public dockets on the Internet at *http://dms.dot.gov.*

Availability of Rulemaking Document

You can get an electronic copy of this document as well as other documents associated with this rulemaking on the Internet by—

(1) Searching the Department of Transportation's electronic Docket Management System (DMS) web page (*http://dms.dot.gov/search*);

(2) Accessing the Government Printing Office's web page at *http://www.gpoaccess.gov/fr/index.html;* or

(3) Visiting TSA's Security Regulations web page at *http://www.tsa.gov* and accessing the link for ''Research Center'' at the top of the page.

Abbreviations and Terms Used in This Document

ALJ—Administrative Law Judge
AMS—Area Maritime Security
ASP—Alternative Security Program
CBP—Bureau of Customs and Border Protection
CDC—Certain Dangerous Cargo
CDL—Commercial drivers license
CDLIS—Commercial drivers license information system
CHRC—Criminal history records check
CJIS—Criminal Justice Information Services Division
COR—Certificate of Registry
COTP—Captain of the Port
DHS—Department of Homeland Security
DOJ—Department of Justice
DOT—Department of Transportation
FBI—Federal Bureau of Investigation
FMCSA—Federal Motor Carrier Safety Administration
FMSC—Federal Maritime Security Coordinator
FSP—Facility Security Plan
HME—Hazardous materials endorsement
HSA—Homeland Security Act
HSPD 12—Homeland Security Presidential Directive 12
MARSEC—Maritime Security
MMD—Merchant Mariner's Document
MSC—Marine Safety Center
MTSA—Maritime Transportation Security Act
NIST—National Institute of Standards and Technology

[1] ''Sensitive Security Information'' or ''SSI'' is information obtained or developed in the conduct of security activities, the disclsoure 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.

NPRM—Notice of Proposed Rulemaking
NVIC—Navigation and Vessel Inspection Circular
OCS—Outer Continental Shelf
REC—Regional Examination Center
SAFETEA–LU—Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users
STCW—International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers, 1978, as amended
TSA—Transportation Security Administration
TPS—Temporary Protected Status
TWIC—Transportation Worker Identification Credential
VSP—Vessel Security Plan

Table of Contents

I. Background
II. Final Rule
A. Coast Guard Provisions
B. TSA Provisions
C. Changes From NPRM
D. Anticipated Future Notices and Rulemaking
E. Summary of TWIC Process under the Final Rule
F. SAFE Port Act of 2006
III. Discussion of Comments
A. Requests for Extension of Comment Period and Additional Public Meetings
B. Coast Guard Provisions
1. Definitions
2. General Comments on Applicability
3. Coast Guard Roles
4. Owner/operator Requirements
5. Requirements for Security Officers and Personnel
6. Recordkeeping/Tracking Persons on Vessels/Security Incident Procedures
7. Reader Requirements/Biometric Verification/TWIC Validation Procedures
8. Access Control Issues
9. TWIC Addendum
10. Compliance Dates
11. General Compliance Issues
12. Additional Requirements—Cruise Ships
13. Additional Requirements—Cruise Ship Terminals
14. Additional Requirements—CDC Facilities
15. Additional Requirements—Barge Fleeting Facilities
16. Miscellaneous
C. TSA Provisions
1. Technology Concerns
2. Enrollment Issues
3. Appeal and Waiver Issues
4. TSA Inspection
5. Security Threat Assessment
6. Immigration Status
7. Mental Incapacity
8. TWIC Expiration and Renewal Periods
9. Fees for TWIC
10. Implementing TWIC in Other Modes
D. Comments Relating to Economic Issues
E. Comments Beyond the Scope of the Rule
IV. Advisory Committee Recommendations and Responses
V. Rulemaking Analyses and Notices
A. Regulatory Planning and Review (Executive Order 12866)
B. Small Entities
C. Assistance for Small Entities
D. Collection of Information
E. Federalism (Executive Order 13132)
F. Unfunded Mandates Reform Act
G. Taking of Private Property
H. Civil Justice Reform
I. Protection of Children
J. Indian Tribal Governments
K. Energy Effects
L. Technical Standards
M. Environment
VI. Solicitation of Comments

I. Background

The Department of Homeland Security (DHS), through the United States Coast Guard (Coast Guard) and the Transportation Security Administration (TSA), issues this final rule pursuant to the Maritime Transportation Security Act (MTSA), Pub. L. 107–295, 116 Stat. 2064 (November 25, 2002), and the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub. L. 109–347 (October 13, 2006). Section 102 of MTSA (46 U.S.C. 70105) requires DHS to issue regulations to prevent individuals from entering secure areas of vessels or MTSA-regulated port facilities unless such individuals hold transportation security cards issued under section 102 and are authorized to be in the secure areas. An individual who does not hold the required transportation security card, but who is otherwise authorized to be in the secure area in accordance with the facility's security plan, must be accompanied by another individual who holds a transportation security card. MTSA also requires all credentialed merchant mariners to hold these transportation security cards, and requires DHS to establish a waiver and appeals process for persons found to be ineligible for the required transportation security card. The SAFE Port Act contained amendments to the basic MTSA requirements for credentialing (concurrent processing, fees, card readers, program roll out, testing and timelines) as well as added new requirements (disqualifying crimes, new hire provisions and discretion as to who may obtain a TWIC). The substance of the SAFE Port Act is discussed in greater detail later in this document.

On May 22, 2006, TSA and the Coast Guard issued a joint notice of proposed rulemaking (71 FR 29396), setting forth the proposed requirements and processes required under sec. 102 of MTSA (TWIC NPRM) for implementation of the TWIC program in the maritime sector. The NPRM proposed changes to three titles of TSA and Coast Guard regulations (33 CFR, 46 CFR, and 49 CFR). The Department intends for these combined changes to increase port security by requiring all credentialed mariners and all persons who require unescorted access to a regulated facility or vessel to have undergone a security threat assessment by TSA and obtain a TWIC.[2] The proposed security threat assessment included a review of criminal, immigration, and pertinent intelligence records. TSA also proposed a process for individuals denied TWICs to appeal adverse determinations or apply for waivers of the standards.

Prior to the publication of the TWIC NPRM, the Coast Guard published a Notice in the **Federal Register** informing the public that the Commandant of the Coast Guard, pursuant to his authority under 50 U.S.C. 191 and 33 CFR part 125, was exercising his authority to require identification credentials for persons seeking access to waterfront facilities and to port and harbor areas, including vessels and harbor craft in such areas. 71 FR 25066 (April 28, 2006). This action has served as an interim measure to improve security at our nation's ports by verifying maritime workers' identities, validating their background information, and accounting for access for authorized personnel to transportation facilities, vessels and activities. *Id.*

The May 22, 2006 TWIC NPRM provided the draft regulatory text for review and solicited public comments for 45 days. TSA and the Coast Guard also held four public meetings throughout the country to solicit public comments. Those meetings were held on May 31, 2006 in Newark, New Jersey; on June 1, 2006 in Tampa, Florida; on June 6, 2006 in St. Louis, Missouri; and on June 7, 2006 in Long Beach, California. Approximately 1200 people attended these meetings. The public can view transcripts of the four public meetings on the public docket for this rulemaking action at *www.regulations.gov.* DHS also received approximately 1770 written comments on the TWIC NPRM. Those comments also can be accessed through the public docket for this action. TSA and the Coast Guard respond to the comments received in the ''Discussion of Comments'' section, below.

Many commenters requested an extension of the comment period and additional public meetings. As explained more fully in the ''Discussion of Comments'' section below, DHS has decided not to delay implementation of the TWIC program by extending the

[2] Additional information on the statutory and regulatory history of this rule can be found in the NPRM at 71 FR 29396 (May 22, 2006).

comment period or providing additional public meetings because it is imperative to begin implementation of the TWIC requirements, and accompanying security threat assessments, as soon as possible to improve the security of our Nation's vessels and port facilities. TSA and Coast Guard, however, have not promulgated in this final rule the proposed requirements on owners and operators relating to biometric readers. The Department will address those proposed requirements, which generated the majority of the comments received on the NPRM, in a separate rulemaking action. Interested parties will have the opportunity to comment on those provisions during that rulemaking action. Although the card reader requirements are not being implemented under this final rule, Coast Guard personnel will periodically, and without advance notice, use handheld readers to check the biometric information contained in the card to confirm the identity of the holder of the TWIC.

On May 22, 2006, the Coast Guard also published a related proposed rule, ''Consolidation of Merchant Mariner Qualification Credentials,'' at 71 FR 29462 (MMC NPRM), proposing the consolidation of Coast Guard-issued merchant mariner's document (MMD), merchant mariner's license (license), certificate of registry (COR) and International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) certificate into a single credential called the merchant mariner credential (MMC). The MMC NPRM proposed to streamline the application process, and reduce the administrative burden for the public and the Federal Government. The public meetings held on the TWIC NPRM also included time for the Coast Guard to receive comments on the MMC NPRM. In a separate rulemaking action published elsewhere in this edition of the **Federal Register**, the Coast Guard has provided a Supplemental Notice of Proposed Rulemaking (SNPRM) also entitled ''Consolidation of Merchant Mariner Qualification Credentials.'' The purpose of the SNPRM is to address comments received from the public on the MMC NPRM, revise the proposed rule based on those comments, and provide the public with an additional opportunity to comment on the revised rulemaking. If it becomes final, the MMC rulemaking is not expected to go into effect until the initial TWIC roll out is complete. This time lapse will not cause a detrimental effect on security, as all credentialed mariners will still need to comply with the TWIC requirements and compliance deadlines set forth in this final rule.

II. Final Rule

Under this final rule, DHS, through the Coast Guard and TSA, requires all credentialed merchant mariners and individuals with unescorted access to secure areas of a regulated facility or vessel to obtain a Transportation Worker Identification Credential (TWIC).

A. Coast Guard Provisions

Owners/operators of MTSA-regulated vessels, facilities, and Outer Continental Shelf (OCS) facilities will need to change their existing access control procedures to ensure that merchant mariners and any other individual seeking unescorted access to a secure area of their vessel or facility has a TWIC.

B. TSA Provisions

Workers must provide biographic and biometric information to apply for a TWIC and pay a fee of $107–$159 to cover all costs associated with the TWIC program. A TWIC applicant must complete a TSA security threat assessment and will be disqualified from obtaining a TWIC if he or she has been convicted or incarcerated for certain crimes within prescribed time periods, lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes or mental incapacity, or are aliens in Temporary Protected Status (TPS). Applicants who seek a waiver and are denied may seek review by an administrative law judge (ALJ). In addition, applicants who are disqualified under § 1572.107 may seek ALJ review of the disqualification.

A security threat assessment is valid for five years. Therefore, in most cases, a TWIC is valid for five years unless a disqualifying event occurs. If an applicant obtains a TWIC based on a comparable threat assessment under § 1572.5(e), the TWIC will expire five years from the date on the credential associated with the comparable threat assessment. To renew a TWIC, the renewal applicant must provide new biographic and biometric information, complete a new threat assessment, and pay the fee to renew the credential.

C. Changes From NPRM

Each of the changes made from the NPRM to the final rule is summarized in Table 1 and discussed in detail following the table.

TABLE 1.—SUMMARY OF SIGNIFICANT CHANGES BETWEEN MAY 22, 2006 NPRM AND THIS FINAL RULE

Topic	NPRM	Final rule
Access control	Visual identity badge and reader (with biometric verification and validity check at facility/vessel based on MARSEC level).	Visual identity badge; Coast Guard will conduct periodic checks of biometric and validity (second rule for reader requirements).
Escorted access	Definition only	Definition modified to clarify that in restricted areas (33 CFR 101.105), ''escort'' means a side-by-side escort; outside restricted areas, ''escort'' may consist of monitoring.
New hires	Not granted unescorted access to secure areas until successful completion of security threat assessment and card issuance.	Permitted to have limited access for 30 consecutive days if accompanied by TWIC-holder and additional requirements are met.
Passenger access area	Defined only for certain vessels (passenger, ferries, cruise ships).	Passenger access area remains and employee access area for certain vessels added (employee access areas do not apply to cruise ships).
TWIC Addendum and recordkeeping requirements.	Included	Excluded.
Secure area	Definition only	Clarified definition's meaning in preamble, and revised part 105 to allow part 105 facilities to submit FSP amendment to change access control area.

TABLE 1.—SUMMARY OF SIGNIFICANT CHANGES BETWEEN MAY 22, 2006 NPRM AND THIS FINAL RULE—Continued

Topic	NPRM	Final rule
Lost/Stolen/Damaged cards	Access procedures defined in TWIC Addendum.	Specific requirements included in regulation.
AMS Committee members	Need TWIC	Need name-based check or a TWIC.
Vessels in foreign waters	No special provisions	Changed secure area definition to state that at certain specified times, U.S. vessels may not have any secure areas.
Emergency responders	Not specifically addressed	Not required to obtain a TWIC for emergency response.
Voluntary compliance	Offered	Not offered.
Compliance dates	12–18 months after final rule	Phased for facilities by each COTP zone. All mariners and vessels 20 months after the publication date of this final rule.
Disqualifying crimes	Same as those used for HME	Amended; new list will apply for both TWIC and HME.
Administrative law judge (ALJ) review.	Not included	May be used for waiver denials and disqualifications under § 1572.107.
Immigration standards	Limited ability for non-U.S. citizens to obtain TWICs.	Expanded to cover foreign maritime students, and certain professionals and specialists on restricted visas; permitting aliens in TPS to apply for a waiver.
Mental incapacity	Could only be waived by showing court order or letter from institution.	Waiver broadened to allow for ''case-by-case'' determinations.
Fee	$95–$149; card replacement fee $36.	$107–$159; card replacement fee $36, but requesting comment on increasing this fee to $60.

1. Changes From Coast Guard's Proposed Rule

Coast Guard is changing several sections of the proposed rule as a result of comments received and additional analysis. These changes include: (1) Changing the access control procedures to be used with TWICs by removing the reader requirements; (2) revising and clarifying the definition of the term ''escorting;'' (3) adding provisions allowing for access for individuals who are new hires and who have applied for, but not yet received, a TWIC; (4) adding a provision to allow for limited, continued unescorted access for those individuals who report their TWIC as lost, damaged, or stolen; (5) adding a provision to create ''employee access areas'' aboard passenger vessels and ferries; (6) removing the proposed requirement to submit a TWIC Addendum and keep additional records regarding who has been granted access privileges; (7) adding a provision to allow certain facilities to designate smaller portions of their property as their secure area via an amendment to their facility security plan; (8) removing the proposed requirement for all AMS Committee members to hold a TWIC; (9) changing the definition of secure area to state that, at certain times, U.S. vessels may not have any secure areas; (10) adding a provision to allow emergency responders to have unescorted access without a TWIC during emergency situations; (11) removing the provision allowing for voluntary compliance for those vessels and facilities not otherwise required to implement the TWIC requirements; and (12) revising the compliance dates for owners/operators of vessels and facilities.

(a). Reader Requirements

After reviewing the comments (which are summarized below), we determined that implementing the reader requirements as envisioned in the NPRM would not be prudent at this time. As such, we have removed the reader requirements from the final rule, and will be issuing a subsequent NPRM to address these requirements. That NPRM will address many of the comments and concerns regarding technology that were raised in the below-summarized comments. We will, however, continue to require the use of the TWIC. As stated in the NPRM, there are considerable security benefits to be gained from a TWIC, even in the absence of reader usage. The TWIC provides greater reliability than existing visual identity badge systems because it presents a uniform appearance with embedded features on the face of the credential that make it difficult to forge or alter. When presented with a TWIC, security personnel familiar with its security features are immediately able to notice any absence or destruction of these features, making it less likely that an individual will be able to gain unescorted access to secure areas using a forged or altered TWIC. Additionally, the Coast Guard will conduct unannounced checks of the cards while visiting facilities and vessels. The Coast Guard will use handheld readers to check the biometrics on the card against the person presenting the card. These unannounced checks are an important component of the security efforts at the ports.

(b). ''Escorting''/''Unescorted Access''

We have amended the definition of escorted access to clarify our intent. Namely, that the distinction between escort and unescorted access are to serve as performance standards, rather than strict definitions. We expect that, when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, physical side-by-side escort. Whether it must be a one-to-one escort, or whether there can be one escort for multiple persons, will depend on the specifics of each vessel and/or facility. We will provide additional guidance on what these specifics might be in a Navigation and Vessel Inspection Circular (NVIC). Outside of restricted areas, however, side-by-side escorting is not required, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted. Again, we will provide additional guidance with more specifics in a NVIC.

(c). New Hires

We have added a new section within parts 104, 105, and 106 to provide owners/operators with the ability to put new hires to work once new hires have applied for their TWIC and an initial name-based check is completed. In order to ensure adequate security for the vessel and facility during this period, these provisions allow new hires to have access to secure areas for up to 30 consecutive days, so long as they pass a TSA name based check and are

accompanied by another employee with a TWIC. If TSA does not act upon a TWIC application within 30 days, the Coast Guard may further extend access to secure areas for another 30 days. Additional guidance on the manner in which new hires may be accompanied will be issued by the Coast Guard. The guidance will be in the form of a NVIC that considers vessel or facility size, crew or staff size, vessel or facility configuration, the number of TWIC holders, and other appropriate factors, or by making a determination on a case-by-case basis. For example, in some instances, where the operating environment of the vessel is such that there is a small crew, and there is a 24-hour live watchstand while underway, we expect to view the new hires as accompanied when the vessel owner/operator ensures that the security measures for monitoring and access control included within their Coast Guard-approved security plans are implemented. As the operating environment increases or becomes more complex, such as might be the case when Certain Dangerous Cargoes (CDCs) are present, we expect to require additional security measures to ensure that the new hires are, in fact, accompanied by an individual with a TWIC. Similar guidance will also be in place for larger vessels, as well as for facilities and OCS facilities. The NVIC will be released in the near future.

In order to take advantage of this new hire provision, the following procedures must be followed:

(1) The new hire will need to have applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process and paying the user fee. He or she cannot be engaged in a waiver or appeal process. The owner or operator must have the new hire sign a statement affirming this.

(2) The owner or operator or the security officer must enter the following information on the new hire into the Coast Guard's Homeport Web site (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment;

(3) The new hire must present an identification credential that meets the requirements of § 101.515 of this subchapter; and

(4) There must be no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the owner or operator or Facility Security Officer (FSO) must not have been informed by the cognizant COTP that the individual poses a security threat.

This provision only applies to direct hires of the owner/operator; it cannot be used to allow temporary unescorted access to contractors, vendors, longshoremen, truck drivers (unless they are direct employees of the owner/operator), or any other visitor. This provision does not apply if the new hire is a Company, Vessel, or Facility Security Officer, or is otherwise tasked with security duties as a primary assignment.

In order for the Coast Guard and TSA to verify that a new hire who is awaiting TWIC issuance passes an initial security review, this provision includes a requirement for the owner, operator, Vessel Security Officer (VSO) or FSO to enter new hire identifying information into the Coast Guard's Homeport web page. The Homeport web page is a secure location capable of communicating sensitive security information such as Vessel Security Plans (VSP) and Facility Security Plans (FSP) between industry and the Coast Guard. The Homeport web page address is *http://homeport.uscg.mil.* Homeport will then interface with the TSA system, and if a match to an enrollment record can be made, the TSA system will pass back to Homeport the result of the initial name-based check. If the result is that the new hire has been cleared, the owner/operator/security officer can put the new hire to work under the provisions of this section and any guidance provided by the Coast Guard in a forthcoming NVIC.

TSA will begin the security threat assessment process as soon as the enrollment record is complete. Generally, TSA can complete an initial security review within 48–72 hours based on all of the information provided during enrollment. Thus, in some cases (where the new hire information is entered into Homeport three or more days following enrollment), the owner/operator/security officer will not have to wait long before finding out if an individual has cleared the initial name check. We expect that Homeport will be able to notify owners/operators/security officers, via e-mail, when it has received an update on any of the new hires entered by that owner/operator/security officer, which will alleviate any need for them to continuously check in with Homeport.

The new hire must have applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process and paying the user fee. The owner/operator must have the new hire sign a statement affirming the enrollment, payment, and that the new hire is not involved in an appeal or waiver application. The owner/operator must retain this statement until the new hire receives a TWIC. The statement must be produced if the Coast Guard requests it during an inspection or investigation. The new hire must also present to the owner or operator a form of identification that meets the standard set in 33 CFR 101.515.

It is also important to note here that a new hire may be initially cleared to work in the secure area under the provisions of this section, but be disqualified from receiving a TWIC when the full threat assessment is complete. The results of the criminal history records check (CHRC) generally will not be fully adjudicated within three days, and if the adjudication reveals a disqualifying criminal history, the new hire will not be cleared to receive a TWIC.

The owner/operator of regulated vessels or facilities is required to accompany new hires in secure areas, which includes monitoring new hires while they are in restricted areas of the vessel or facility. Monitoring has the same meaning here as found in §§ 104.285, 105.275, and 106.275 of 33 CFR chapter I, subchapter H.

We are also requiring owners/operators of regulated vessels and facilities to determine that their new hires need access to secure areas immediately in order to prevent adverse impact to the operation of the vessel or facility. Owners and operators must identify that a hardship exists to their operations if their new hires are not allowed access. This adverse impact is not the impact of simply providing escorts for new hires, but must be adverse impacts to the business itself from not being able to employ new hires immediately in secure areas without escort.

Owners and operators of regulated vessels and facilities must be assured that there are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC. This information can come through the normal hiring process, reference checks, or interviews. Also, if the Coast Guard, through its Captain of the Port (COTP), has informed the owner/operator that the new hire poses a security threat, the new hire may not have unescorted access to secure areas of the vessel or facility. Only individuals who pass a threat assessment and are issued a TWIC may have unescorted access to secure areas of the vessel or facility.

(d). Access for Individuals With Lost/Stolen TWICs

Under the NPRM, we proposed requiring owners/operators to include alternative security procedures in the TWIC Addenda. These alternative procedures were to be used in various situations, such as when individuals needed unescorted access to secure areas but had lost their TWIC, had it stolen, or simply forgotten it that day. As discussed below, we removed the TWIC Addendum requirement from the final rule, but we wanted to include a provision to allow TWIC holders to continue, for a short period, to have unescorted access to secure areas after reporting their TWICs as lost, damaged, or stolen. As a result, this final rule includes specific procedures for owners/operators to use in the case of lost, damaged, or stolen TWICs. This procedure includes having the individual report his/her card as lost, damaged, or stolen to the TWIC Call Center and checking another form of identification that meets 33 CFR 101.515, provided there are no other suspicious circumstances that would cause an owner/operator to question the veracity of the individual. In order to prevent this procedure from becoming a significant loophole in the TWIC regulation, we require that the individual be known to have had a valid TWIC and to have previously been granted unescorted access, and have limited the use of the procedure to seven (7) consecutive calendar days. This should provide enough time for the replacement card to be produced and shipped to the nearest enrollment enter, and for the individual to travel to that center to pick up the replacement card.

(e). ''Employee Access Areas''

We intended for the term ''passenger access area'' to capture those employees whose jobs are necessary solely for the entertainment of the passengers of the vessel, such as musicians, wait staff, or casino employees on a passenger vessel. Upon reviewing comments, however, we realized that there are a variety of employees who may need to enter non-passenger spaces, such as the galley, who would be included under TWIC's applicability merely because of their need to enter these areas. As such, we are adding a definition for ''employee access areas,'' for use only by passenger vessels and ferries. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the vessel security plan (VSP). Note, however, that any employee that needs to have unescorted access to areas of the vessel outside of the passenger or employee access areas will need to obtain a TWIC.

(f) TWIC Addendum and Recordkeeping Requirements

We removed the TWIC Addendum requirement from the final rule when we determined that the reader requirements would be delayed until a subsequent rulemaking. The purpose of the TWIC Addendum was to allow the owner/operator to explain how the readers would be incorporated into their overall access control structure, within the standards provided in the NPRM. With the removal of the reader requirements from this final rule, we feel it is appropriate to also remove the TWIC Addendum requirement. Additionally, because we envision the TWIC Addendum to be a part of the subsequent rulemaking on reader requirements, we felt it would be overly burdensome to also require a TWIC Addendum at this point in time.

The recordkeeping requirements related to TWIC implementation have also been removed from the final rule. We had proposed the requirements because we believed they could be satisfied by using the TWIC readers, which were also proposed. Due to our decision to remove the reader requirements from this final rule, it makes sense to also remove the recordkeeping requirements that were intrinsically tied to those readers.

(g). Secure Area

We did not intend for the terms ''secure area'' and ''restricted area'' to be read as meaning the same thing. Restricted areas are defined already in the MTSA regulations as ''the infrastructure or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection.'' (33 CFR 101.105) Additionally, those regulations spell out certain areas within vessels and facilities that must be included as restricted areas (*see* 33 CFR 104.270, 105.260, and 106.265). This final rule defines ''secure area'' as meaning the area over which an owner/operator has implemented security measures for access control. In other words, the secure area would be anything inside the outer-most access control point of a facility, and it would encompass the entirety of a vessel or OCS facility.

We adopted this definition after much consideration, including consideration of making only restricted areas secure areas. We ultimately abandoned this option, however, when we realized that equating the restricted area to the secure area would have required that the readers and biometric verification be used at the entry points of each restricted area. Because some facilities and vessels have multiple restricted areas that are not always contiguous, this would have likely meant that many owners/operators would have needed more than one reader, increasing their compliance costs. Additionally, the process of repeated biometric identification could have interfered with the operations of facilities and vessels. Finally, we determined that there are areas within some facilities that are not required to be restricted areas that should be deemed secure areas, such as truck staging areas, empty container storage areas, and roads leading between the facility gates and the pier. Allowing persons who have not been through the security threat assessment or are not escorted to have access to these areas could provide them with the opportunity to access the non-restricted areas of the facility to perpetrate a transportation security incident (TSI). Pushing the secure area out beyond the restricted area makes the event of an intentional TSI less likely. As a result, we decided to define the secure area as the ''access control area,'' thus limiting the number of readers required, as well as the number of times biometric verification would need to take place, and providing for the necessary level of security outside of restricted areas. We note, however, that facility owners/operators have the discretion to designate their entire facility as a restricted area. In this situation, the restricted area and secure area would be one and the same.

We recognize that many facilities may have areas within their access control area that are not related to maritime transportation, such as areas devoted to manufacturing or refining operations, and were only included within the FSP because the owner/operator did not want to have to install additional access control measures to separate the non-maritime transportation related portions of their facility from the maritime transportation related portions. Given the new obligations of this TWIC final rule, however, these owners/operators may wish to revisit this decision. As such, we are giving facility owners/operators the option of amending their FSP to redefine their secure area, to include only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation

security incident. These amendments must be submitted to the cognizant COTP by July 25, 2007.

We realize that there may be some owners and operators of vessels that would like the same option. However, vessels present a unique security threat over facilities in that they may not only be targets in and of themselves, but may also be used as a weapon. Due to this fact, we will continue to define the entire vessel as a ''secure area,'' making exception only for those special passenger and employee access areas which are discussed above. Vessel owners/operators need not submit an amendment to the VSP in order to implement these special areas, however they may do so, following the procedures described in part 104.

(h). U.S. Vessels in Foreign Waters

Due in part to the unique operating requirements imposed on U.S. Offshore Supply Vessels (OSVs) and Mobile Offshore Drilling Units (MODUs) when operating in support of OCS facilities in foreign waters, we determined that we must change some language from the proposed rule. As such, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provision in 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. The effect of this change is to exempt these vessels from the TWIC requirement while they are operating under the referenced waivers. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

(i). Area Maritime Security (AMS) Committee Members

The NPRM proposed requiring all members of AMS Committees to have a TWIC. We recognize that large numbers of the members will either (1) already have a TWIC, due to their role within the security organization of a facility, or (2) already have undergone some type of comparable background screening due to their position as a Federal, State, or local law enforcement official. After further consideration, we believe that anyone not falling into one of these categories could be discouraged from volunteering to sit on an AMS Committee, due to the cost of obtaining a TWIC. This could have a detrimental effect on the AMS Committee, as there may be individuals who are experts in security who would be (and in some cases already are) valuable parts of AMS Committees, who would opt out of sitting on the Committee rather than assume the cost of obtaining a TWIC. Therefore, we have changed the final rule to allow AMSC members to serve on the AMSC after the completion of a name-based terrorist check from TSA. If an AMSC member requires unescorted access to secure areas of vessels or facilities they will be required to obtain a TWIC. If, however, they do not require unescorted access, but do need access to SSI, they must first pass a TSA name based check at no cost to the AMSC member. The Federal Maritime Security Coordinator for the member's particular AMSC (*i.e.* COTPs) will forward the names of these individuals to TSA or Coast Guard Headquarters for clearance prior to sharing SSI with these members.

(j). Emergency Responders

We added a provision within 33 CFR 101.514 to allow State and local emergency responders to gain access to secure areas without a TWIC during an emergency situation. Not all emergency responders will fall into the category of State or local officials. We feel it is imperative that these individuals be allowed unescorted access to secure areas in an emergency situation. Emergency responders who are not State or local officials are encouraged to apply for a TWIC. Under the existing access control requirements of 33 CFR 105.255, the owner or operator has documented procedures for checking credentials prior to allowing access and will maintain responsibility for all those granted access to a vessel or facility, even in an emergency situation.

(k). Voluntary Compliance

The provisions that would have allowed vessel and facility owners/operators to implement voluntary TWIC programs have been removed. These provisions have been eliminated due to the fact that neither TSA nor the Coast Guard can, at this time, envision being in a position to approve voluntary compliance before the full TWIC program, (*i.e.*, reader requirements) is in place. We will keep it in mind, however, as we develop our NPRM to repropose reader requirements.

(l). Compliance Dates

We have also revised the compliance dates slightly. Vessels will now have 20 months from the publication date of this final rule to implement the new TWIC access control provisions. Facilities will still have their compliance date tied to the completion of initial enrollment in the COTP zone where the facility is located. This date will vary, and will be announced for each COTP zone at least 90 days in advance by a Notice published in the **Federal Register**. The latest date by which facilities can expect to be required to comply will be September 25, 2008. Additionally, mariners will not need to hold a TWIC until September 25, 2008. Mariners may rely upon their Coast Guard-issued credential and a photo ID to gain unescorted access to secure areas to any facility that has a compliance date earlier than September 25, 2008.

2. Changes From TSA's Proposed Rule

TSA is changing several sections of the proposed rule as a result of comments received, new legislation, and additional analysis. The changes include: (1) Establishing procedures for review of waiver denials by an ALJ; (2) applying the hazmat and TWIC appeal procedures to air cargo personnel; (3) amending the list of disqualifying criminal offenses; (4) expanding the group of aliens who meet the immigration standards; (5) amending the waiver standards for applicants disqualified due to mental incapacity; (6) amending the fees for TWIC; (7) revising the standard for drivers licensed in Mexico and Canada who transport hazardous materials into and within the United States; and (8) modifying the prohibitions on fraudulent use or manufacture of TWIC or access control procedures.

(a). Review by Administrative Law Judge

We noted in the NPRM that if legislation was enacted after publication of the final rule to require review by an Administrative Law Judge of the denial of waiver requests by TSA, we would include such a statutory mandate in the final rule. *See* 71 FR at 29421. The Coast Guard and Maritime Transportation Act of 2006, Pub. L. 109–241, was enacted on July 11, 2006. Section 309 of this Act requires the Secretary of Homeland Security to establish an ALJ review process for individuals denied a waiver by TSA. Accordingly, we are including the ALJ review procedures in new § 1515.11.

The ALJ review process set forth under § 1515.11 does not alter the substantive criteria under which TSA will grant or deny a waiver. Therefore, this provision constitutes a rule of agency procedure and may be implemented without prior notice and comment under the Administrative Procedure Act, 5 U.S.C. 553(b)(A). *See Hurson Assoc. Inc.,* v. *Glickman,* 229 F.3d 277 (D.C. Cir. 2000) (rule eliminating face-to-face process in agency review of requests for approval

was procedural and not subject to notice-and-comment rulemaking).

The new legislation requires ALJ review to be available for denials of waivers. Under the rules waivers are not available for determinations under § 1572.107 that an applicant poses a security threat, which usually is based on an intelligence-related check involving classified information. However, we have considered that there appears to be an intent that we provide for an ALJ review of such determinations, considering, for example, that the statute provides for ALJ review of classified information, which rarely is relevant to waivers under the current rules. We have also considered that the decision to determine whether an applicant poses a threat under § 1572.107 is largely a subjective judgment based on many facts and circumstances. The same is true for the decision to grant or deny a waiver of the standards in §§ 1572.103 (criminal offenses), aliens who are in TPS under 1572.105, or 1572.109 (mental capacity). Accordingly, we are providing for ALJ review of both a determination that the applicant does not meet the standards in § 1572.107, and a denial of a waiver of certain standards in §§ 1572.103, 1572.105, and 1572.109.

An applicant who has received an Initial Determination of Threat Assessment based on § 1572.107 may first appeal that determination using the procedures in new § 1515.9. If after that appeal TSA continues its determination that the applicant is not qualified, the applicant may seek ALJ review under § 1515.11.

On the other hand, the determination that an applicant does or does not have a disqualifying criminal offense listed in § 1572.103, immigration status in § 1572.105, or mental capacity described in § 1572.109, largely involves an analysis of the legal events that have occurred. Such analyses depend mainly on review of legal documents. We have retained in § 1515.5 the paper hearing process for the appeal of an Initial Determination that an applicant is not qualified under those sections. At the end of that appeal, if TSA issues a Final Determination that the applicant is not qualified under one of those sections, the applicant may seek review in the Court of Appeals. At any time, however, the applicant may seek a waiver of certain standards in those sections on the basis that, notwithstanding a lack of qualification, the applicant asserts that he or she does not pose a security threat and thus seeks to waive the subject standards. The applicant initiates the request for a waiver using the procedures in § 1515.7. If a waiver is not granted, the applicant may seek review by an ALJ under § 1515.11.

For consistency, we are providing the same review processes for hazardous materials endorsement (HME) applicants that we are providing for TWIC applicants.

Paragraph 1515.11(a) of this new section specifies that the new process applies to applicants who are seeking review of an initial decision by TSA denying a request for a waiver under § 1515.7 or who are seeking review of a Final Determination of Threat Assessment issued under § 1515.9.

Section 1515.11(b) allows the applicant 30 calendar days from the date of service of the determination to request a review. The review will be conducted by an ALJ who possesses the appropriate security clearances to review classified information. The rule sets forth the information that the applicant must submit. This section clarifies that the ALJ may only consider evidence that was presented to TSA at the time of application in the request for a waiver or the appeal. If the applicant has new evidence or information to support a request for waiver, the applicant must file a new request for a waiver under § 1515.7 or a new appeal under § 1515.9 and the pending request for review will be dismissed. Section 1515.11 provides detailed requirements for the conduct of the review, such as requests for extension of time and duties of the ALJ.

In accordance with the Coast Guard and Maritime Transportation Act, this section provides for ALJ review of classified information on an *ex parte*, in camera basis and consideration of such information in rendering a decision if the information appears to be material and relevant.

Paragraph 1515.11(f) provides that within 30 calendar days after the conclusion of the hearing, the ALJ will issue an unclassified decision to the parties. The ALJ may issue a classified decision to TSA. The ALJ may decide that the decision was supported by substantial evidence on the record or that the decision was not supported by substantial evidence on the record. If neither party requests a review of the ALJ's decision, TSA will issue a final order either granting or denying the waiver or the appeal.

Paragraph 1515.11(g) describes the process by which a party may petition for review of the ALJ's decision to the TSA Final Decision Maker. The TSA Final Decision Maker will issue a written decision within 30 calendar days after receipt of the petition or receipt of the other party's response. The TSA Final Decision Maker may issue an unclassified opinion to the parties and a classified opinion to TSA. The decision of the TSA Final Decision Maker is a final agency order.

Paragraph 1515.11(h) states that an applicant may seek judicial review of a final order of the TSA Final Decision Maker in accordance with 49 U.S.C. 46110, which provides for review in the United States Court of Appeals. Under sec. 46110 a party has 60 days after the date of service of the final order to petition for review.

(b). Appeal Procedures for Air Cargo Personnel

In the final rule we are adding the appeal procedures that currently apply to air cargo workers codified at 49 CFR parts 1540 to 1515. In the NPRM TSA stated that it may use the procedures in part 1515 for other security threat assessments, such as for air cargo personnel. *See* 71 FR at 29418. At that time the air cargo proposed rule had been published but was not yet final, and it proposed to use appeal procedures that were essentially the same as for HME applicants. The air cargo rule has now been made final. *See* 71 FR 30478 (May 26, 2006). Because part 1515 was not yet final in the air cargo rule, we placed the appeal procedures for the air cargo security threat assessment into part 1540 subpart C, along with other procedures that apply to air cargo threat assessments. In a further effort to harmonize security threat assessments, we are now moving the appeal procedures for air cargo personnel to part 1515. For consistency with the TWIC and HME processes we are providing for review by an ALJ as described above.

We are also revising part 1540 subpart C to harmonize more with part 1572. Thus, we are replacing ''individual'' with ''applicant'' to refer to the person who is applying for a security threat assessment. We are also revising § 1540.205 to read essentially the same as § 1572.21 for TWIC, because it serves the same function. Note that while the procedures for TWIC refer to CHRCs and other checks, the procedures for air cargo personnel refer only to intelligence-related checks, because they are not subject to the other checks conducted on TWIC applicants.

(c). Disqualifying Criminal Offenses.

In this final rule, the list of criminal acts that disqualify an applicant from holding an HME under 49 CFR 1572.103 now applies to TWIC applicants. We believe equal treatment for transportation workers is appropriate and consistent with the pertinent

statutory requirements. The standards for the HME rule were mandated by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) Pub. L. 107–56, 115 Stat.272 (October 25, 2001). It provides that TSA conduct a security threat assessment on applicants to determine if they pose a ''security risk.'' The USA Patriot Act was enacted shortly after and in response to the terrorist attacks on the United States on September 11. As a result, we interpreted the language ''security risk'' to mean a risk of terrorism or terrorist activity. Nothing in the statute or the legislative history of the USA Patriot Act contradicts this reading of the language. MTSA, enacted a year later, requires a security threat assessment to determine whether an applicant poses a ''terrorism security threat.'' We believe the security threat assessment required under MTSA is the same threat assessment required under the USA Patriot Act, even though the actual language differs slightly.

In addition, TSA is making administrative and substantive changes to this section. In the NPRM, TSA indicated that it was considering changing the list of disqualifying crimes and asked for comment on the list. TSA received significant comments from Congress and others suggesting that the list of disqualifying crimes is overly broad, and that some crimes had more of a nexus to terrorism than others. 152 Cong. Rec. 2120 (2006). *See also* Comments of House Committee on Homeland Security on TSA and Coast Guard's Rule to Implement TWIC, July 6, 2006. TSA has evaluated the list of disqualifying crimes and decided to fine tune the list to better reflect crimes that are more likely to result in a terrorism security risk or a transportation security incident, and thus should disqualify an applicant from receiving a TWIC.

TSA is making a substantive change to this section concerning the crimes of treason, sedition, espionage, and terrorism listed in § 1572.103(a), which are permanently disqualifying. Applicants convicted of these crimes are not eligible for a waiver. As we proposed to do in the NPRM, TSA is adding conspiracy to commit these crimes to the list of crimes that are not subject to a waiver request. TSA has determined that a conviction of conspiracy to commit espionage, treason, sedition, or terrorism is indicative of a serious, ongoing, unacceptable risk to security and should not be waived under any circumstances.

TSA is changing the language in (a)(4) from ''a crime listed in 18 U.S.C. Chapter 113B—Terrorism'' to ''a federal crime of terrorism as defined in 18 U.S.C. 2332b(g)'' or conspiracy to commit such crime, or comparable State law. Section 2332b(g) is a definitional list that is broader and more explicit than the crimes punished directly in Chapter 113B. We are making this change to more accurately capture all pertinent terrorism-related crimes. Although we intended to be as inclusive as possible with the previous language, experts at the Department of Justice advise that the new language more accurately captures the relevant criminal acts. TSA is adding felony bomb threat in paragraph (a)(9) as a permanent disqualifier including maliciously conveying false information concerning the deliverance, placement, or detonation of an explosive or other lethal device against a state or government facility, public transportation system or an infrastructure facility. TSA is including this crime because it is, in essence, a threat to commit an act of terrorism. We note that we have disqualified an applicant with such crime under the authority of current paragraph (b)(6) dishonesty, misrepresentation, or fraud. To be clear that this crime is a permanent disqualifier, we are adding it as an independent offense in § 1572.103(a)(9). This offense includes making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility.

Paragraph 1572.103(a)(9) is based in part on conduct prohibited by several federal crimes. The first is 18 U.S.C. 844(e), which is found in chapter 40 (Explosive Materials) of the federal criminal code. Section 844(e) criminalizes the use of the mail, telephone, or other instrument of interstate or foreign commerce to willfully make any threat or maliciously convey false information knowing the same to be false, concerning an attempt to kill, injure, or intimidate any individual or unlawfully damage or destroy any building, vehicle, or other real or personal property by means of an explosive. This crime is already disqualifying under paragraph (a)(7). For inclusion in the list of disqualifying crimes, TSA modified this description to broaden it beyond a threat made through an instrument of interstate or foreign commerce. This change provides a disqualification for purely intrastate conduct that results in a felony conviction under State law. TSA also modified the wording found in section 844(e) to include threats of use of lethal weapons in addition to fire and explosives, such as biological, chemical, or radiological weapons. Threats to use these weapons are prohibited by other sections of the federal criminal code. *See, e.g.*, 18 U.S.C 175 (Biological weapons); 18 U.S.C. 229 (Chemical Weapons); and 18 U.S.C. 2332h.

TSA has revised the language of paragraph (b) to clarify that the crimes listed are disqualifying if either of the following are true: (1) The applicant's date of conviction is within seven years of the date of application; or (2) the applicant was incarcerated for that crime and was released from incarceration within five years of the date of application.

TSA is adding the offense of fraudulent entry into seaport secure areas to the list of interim disqualifiers. This is a new provision in 18 U.S.C. 1036 that we believe is particularly relevant to this rulemaking and any TWIC applicant.

TSA is also clarifying in paragraph (b)(2)(iii) that money laundering is an interim disqualifier because it is encompassed under the crimes of dishonesty and fraud and can be a means of funding terrorism. It is known that criminals obtain money from the illegal sale of drugs, firearms and other contraband, launder the money to hide its origin and then funnel this money to terrorist groups. The money laundering disqualifier is limited to convictions where the laundering was for proceeds of other disqualifying criminal activities such as drugs or weapon sales.

TSA is also clarifying that welfare fraud and passing bad checks will not be considered crimes of dishonesty, fraud, or misrepresentation for purposes of paragraph (b)(2)(iii). In some states, conviction for passing a bad check of $100 is a felony and so would be disqualifying for an HME or TWIC applicant. Similarly, a conviction for welfare fraud can be a felony under state law, depending on the circumstances of the case. TSA believes that these crimes generally do not have a nexus to terrorism and therefore should not be disqualifying under MTSA.

TSA is moving the definitions of ''explosive,'' ''firearm,'' and ''transportation security incident'' from § 1572.3 to § 1572.103, where the terms are used. This should help to eliminate uncertainty about the crimes that are disqualifying. In addition, TSA is adopting clarifying language concerning the kind of activity that constitutes a ''transportation security incident.'' As required in § 7105 of SAFETEA–LU,

codified at 47 U.S.C. 5103a(g)(3), the definition now makes clear that nonviolent labor-management activity is not considered a disqualifying offense.

The list of disqualifying crimes in § 1572.103 applies equally to TWIC and HME applicants, thus the amendments apply to both.

(d). Immigration standards

The NPRM was drafted to permit non-resident aliens in the U.S. with unrestricted authorization to work here to apply for and obtain a TWIC. As a result of comments and the relatively common employment of foreign specialists in certain maritime job categories who do not have ''unrestricted'' work authorization, we are expanding the group of aliens who can apply to include certain restricted work authorization categories.

For purposes of this discussion, it is helpful to explain that there are two categories of U.S. visas: immigrant and nonimmigrant. As provided in the immigration laws, an immigrant is a foreign national who has been approved for lawful permanent residence in the United States. Immigrants enjoy unrestricted eligibility for employment authorization. Nonimmigrants, on the other hand, are foreign nationals who have permanent residence outside the United States and who are admitted to the United States on a temporary basis. Thus, immigrant visas are issued to qualified persons who intend to live permanently in the United States. Nonimmigrant visas are issued to qualified persons with permanent residence outside the United States, but who are authorized to be in the United States on a temporary basis, usually for tourism, business, study, or short-or long-term work. Certain categories of lawful nonimmigrant visas or status allow for restricted employment authorization during the validity period of the visa or status.

TSA has carefully reconsidered the immigration standards we proposed in the NPRM in light of the comments we received relating to immigration status and our own ongoing analysis. As a result, we are amending the immigration standards for TWIC and HME applicants. The critical issues we examined and on which we rely to determine whether an alien should be permitted to apply for a TWIC or HME are: (1) The statutory language regarding immigration status; (2) the degree to which TSA can complete a thorough threat assessment both initially and perpetually on the applicant; (3) the duration of the applicant's legal status as of the date he or she enrolls and the degree to which we can control possession of a TWIC once legal status ends; (4) the restrictions, if any, that apply to the applicant's immigration status; (5) particular maritime professions that commenters stated often involve aliens; and (6) the checks done by the U.S. Department of State (State Department) or other federal agency relevant to granting alien status.

With respect to non-U.S. citizens, MTSA provides that an individual may not be denied a TWIC unless he or she may be denied admission to or removed from the United States under the Immigration and Nationality Act (8 U.S.C. 1101, *et seq.*), or ''otherwise poses a terrorism security risk to the United States[3].'' 46 U.S.C. 70105(c). Under this final rule, all applicants for TWICs must be lawfully present in the country. Each of the permissible classes listed in § 1572.105 has, as a basis, lawful presence in the United States. Additionally, if the duration of an applicant's legal status as of the date of enrollment does not meet or exceed the period of validity of the credential, five years, we have concerns about permitting the applicant to receive a TWIC[4]. Given the statutory language—that we may deny a TWIC to an applicant who ''*may be* denied admission to the United States or *removed from* the United States under the Immigration and Nationality Act''—we believe it is not advisable and may be inconsistent with MTSA to issue a five-year credential to an individual whose known lawful status as of the date of enrollment is a much shorter time period. The statutory language reflects the evolving nature of immigration status and we believe it is a significant distinction that warrants particular treatment.

Changes to alien status occur frequently and are difficult to track accurately in real time and perpetually, both of which are necessary to ensure that a TWIC holder remains in legal status. Where we can achieve a level of certainty that the applicant will not possess a TWIC longer than his or her lawful presence and commenters have indicated there is a need for certain short-term aliens to hold a TWIC, we will consider issuing them a credential.

Many aliens in lawful nonimmigrant status are not eligible to work in the United States or their employment authorization is restricted in some way, usually to the particular sponsoring employer or entity. With the exception of students in valid M–1 nonimmigrant status who are enrolled in the U.S. Merchant Marine Academy or a comparable State school and must complete vocational training, we do not believe it would be consistent with MTSA to permit lawful nonimmigrants that are ineligible to work or conduct business in the United States to apply for a TWIC. Also, if the employment restriction placed on the nonimmigrant generally prevents the individual from working in a maritime facility or vessel, we do not believe a TWIC should be granted. The final rule now lists the nonimmigrant classifications with restricted employment authorization that have a nexus to the maritime industry. Aliens in these nonimmigrant categories with restricted employment authorization may apply for a TWIC notwithstanding the fact that their immigration status may expire in less than five years, because we are requiring additional measures to ensure that the TWIC expires after the employment that requires unescorted access to secure areas ends.

The final rule now requires employers of TWIC holders who are lawful nonimmigrants with restricted authorization to work to retrieve the applicant's TWIC when the job for which the nonimmigrant status was granted is complete. The employer in this situation should be well aware that the employment status has ended because the visa was issued to facilitate a specific job or employment with the employer. However, if an employer terminates the employment relationship with the alien working on a restricted visa, or that alien quits working for the employer, the employer is required to notify TSA within 5 days and provide the TWIC to TSA if possible. Additionally, all applicants must return their TWIC to TSA when they are no longer qualified for it, and a visa applicant's TWIC expires when either the employment ends or the visa expires. These requirements should minimize the likelihood that an alien will continue to possess a TWIC and have unescorted access to secure areas

[3] The governing statute for immigration standards for an HME (49 U.S.C. 5103a) requires TSA to ''review relevant databases to determine the status of an alien under U.S. immigration law,'' which provides TSA more discretion to determine whether an alien in a particular immigration class should hold an HME. In order to maintain consistent standards among transportation workers where possible, the immigration standards we are establishing in this final rule for TWIC applicants will also apply to HME applicants. However, as a threshold matter, HME applicants must first meet the standards to hold a commercial driver's license promulgated by the U.S. Department of Transportation, which may include immigration status.

[4] The TSA system is not currently programmed to issue credentials with varying expiration dates; all TWICs will expire five years from the date on which they were issued. We plan to explore modifying aspects of the TSA system as the program matures.

of the maritime industry after his or her legal status to do so expires.

The requirement to return a TWIC to TSA when the pertinent employment ends does not apply to employers of lawful nonimmigrants with unrestricted authorization to work or employers of unrestricted lawful nonimmigrants. Under the immigration laws, the status assigned to an alien carries with it the determination that the individual may work in the United States with or without restriction. Where the alien status includes employer sponsorship as a condition of legal presence, we believe it is appropriate to require the employer to return the credential to TSA once that relationship ends. However, in the cases of alien status that do not carry employment restrictions, we do not believe it is advisable at this time to require any employer action. The lawful nonimmigrant who is not under employment restriction may cease working for an employer and maintain legal status. Retrieving the TWIC at this point would not be appropriate. If the applicant loses lawful status, under the rule, he or she must report any disqualifying offense to TSA and surrender the TWIC. In addition, the enrollment record for each applicant contains contact information for employers, and if TSA determines that an applicant has lost legal status, we would generally have the information necessary to contact the employer and the TWIC holder.

To satisfy the second prong of MTSA's immigration status requirement, that a TWIC holder does not pose a terrorism security threat to the United States, TSA considers a variety of factors. TSA must be able to conduct a comprehensive threat assessment of the applicant. As in all of TSA's security threat assessment programs, we will conduct a comprehensive threat assessment of each applicant upon enrollment, and then will vet the applicants perpetually using appropriate databases throughout the five-year term of the TWIC. We consider the initial and perpetual vetting to be equally important in maintaining a high level of confidence in the TWIC population. To the extent that a full threat assessment cannot be completed on an applicant initially or perpetually, TSA has concerns about granting that applicant unescorted access to secure areas of maritime facilities and vessels.

Many immigration statuses change over time, and TSA generally is not in a position to perpetually vet the immigration status of an applicant. We are reluctant to provide a five-year TWIC under these circumstances unless we achieve some level of control over the actual credential through the applicant's employer to minimize the likelihood that an alien who has lost lawful status keeps the credential.

A significant component of a comprehensive security threat assessment is a fingerprint-based criminal history records check for arrests, indictments, wants, warrants, and serious felony convictions. If we are unable to complete such a check because we cannot access the criminal records of the country in which an applicant has lived for many years, we have concerns that we cannot make an accurate assessment of the individual. Many U.S. workers commented on this fact, in some cases asserting that U.S. citizens are held to a higher standard than workers born abroad because of the inability to do a complete criminal records check on foreign-born applicants. We do not believe that this situation alone constitutes justification to deny non-citizens a TWIC, particularly since U.S. citizens may be born abroad, or spend substantial time abroad. However, it does give rise to a legitimate security concern. Consequently, we must make every effort to minimize the likelihood that someone with malicious intent can enter the United States legally or illegally, hide significant prior criminal or terrorist activity, and obtain unescorted access to secure areas of the maritime industry.

To reduce the likelihood that TWICs will be issued to someone with malicious intent, we are changing the immigration standards in a variety of ways to reduce those eligible for TWICs to only those individuals on whom the Department of State and/or DHS can perform an adequate security review. First, we are not permitting certain aliens in lawful nonimmigrant status with unrestricted employment authorization to apply for a TWIC. We are not permitting aliens in valid S–5 or S–6 lawful nonimmigrant status with unrestricted authorization to work in the United States to apply for a TWIC. Individuals who are in S–5 and S–6 lawful nonimmigrant status are informants providing information relating to criminal or terrorist organizations. Typically, individuals who are able to provide this kind of information to law enforcement personnel in the United States have been engaged in criminal or terrorist activity themselves. For this reason, we believe they pose a security risk and should not be granted a TWIC. Additionally, this status is granted to no more than 250 individuals per year, and so the likelihood that preventing these individuals from applying for a TWIC would adversely impact a significant number of applicants or the maritime industry is virtually nonexistent. Finally, the S–5 and S–6 status requires frequent contact with U.S. law enforcement personnel for approximately three years, after which time the applicant may be recommended for lawful permanent resident status. After these individuals satisfy the conditions of their status and become lawful permanent residents, the risk they initially present would effectively be mitigated and they would be permitted to apply for a TWIC.

We do not believe it is advisable to permit lawful nonimmigrants in K–1 or K–2 status to apply for a TWIC. These individuals include the fiancés and minor children of fiancés of U.S. citizens. Their lawful status expires in just four months. We believe these individuals can be escorted under the final rule until they obtain permanent or other lawful status.

Aside from holders of the S–5 and S–6 and K–1 and K–2 statuses all lawful nonimmigrants with unrestricted authorization to work in the United States may apply for a TWIC.

Second, we are revising the rule to treat U.S. nationals, that is, principally American Samoans, as we treat U.S. citizens.[5] We accomplished this change by adding a definition to the rule for ''National of the United States,'' which means a citizen of the United States or an individual who owes permanent allegiance to the United States. This change is consistent with longstanding principles of immigration law and we believe would not introduce a security threat. Similarly, the final rule permits citizens of the Federated States of Micronesia, the Republic of the Marshall Islands, and Palau who have been admitted as nonimmigrants under the Compacts of Free Association between the United States and those countries to apply for a TWIC. The United States has entered into treaties with these countries that afford their citizens preferred treatment. For instance, citizens of these countries may reside indefinitely and work in the United States without restriction. Therefore, we believe it is appropriate to permit these individuals to apply for a TWIC.

Third, in response to many comments about the use of foreign professionals in the maritime industry for specialty work, we are permitting certain lawful

[5] Note that Swains Island has been incorporated into American Samoa and thus does not need a separate reference. (48 USC 1662) In addition, this includes nationals of the Commonwealth of the Northern Mariana Islands.

nonimmigrants with restricted authorization to work in the United States to apply for a TWIC. There is a longstanding practice of employing non-U.S. citizens to complete specialized maritime tasks, such as maintaining vessel engines and motors. In addition, many international maritime companies transfer staff from abroad into the United States for short or long-term periods, and many of these individuals must work at maritime facilities or on vessels. Denying this segment of the industry the opportunity to apply for a TWIC could adversely impact maritime operations and economic vitality. However, to mitigate our concerns about the inability to complete a thorough initial and perpetual threat assessment on individuals who have not lived in the United States for any significant period of time and who are authorized to remain in the United States for less than five years, we are adding requirements for employers and affected workers to return the TWIC to TSA when the job is completed or the worker otherwise ceases employment with the company.

We received a comment concerning aliens who are religious personnel in valid R–1 lawful nonimmigrant status with restricted employment authorization. The commenter noted that vessel crew members may request spiritual guidance or religious services when their vessel docks at a port in the United States, and religious workers in valid R–1 status should be permitted to apply for a TWIC to board the vessel. Seafarer Welfare Advocates are eligible for TWICs as long as they meet the TWIC rulemaking eligibility requirements; however, there are no exemptions for aliens holding R–1 visas. We believe that individuals with R–1 visas can be escorted because any individual providing religious services to crew members on a vessel would be on board the vessel for relatively short periods of time and would most likely be in the company of TWIC holders during that time. While we do not believe that these individuals need to hold a TWIC to carry out their religious or spiritual functions, they may apply and will be issued TWICs if they meet the eligibility requirements.

Fourth, we are permitting students of the United States Maritime Academy and comparable State maritime colleges in valid M–1 lawful nonimmigrant status to apply for a TWIC. These individuals clearly have a need for unescorted access to maritime facilities and vessels as they complete their vocational training in the United States.

Fifth, we are adding individuals who are in TPS to the group of applicants who may apply for a waiver. Temporary Protected Status is a temporary immigration status granted to eligible nationals of designated countries. The Secretary may designate a country for TPS when it is determined that (1) there is an ongoing armed conflict in the state and, due to that conflict, return of nationals to that state would pose a serious threat to their personal safety; (2) the state has suffered an environmental disaster resulting in a substantial, temporary disruption of living conditions, the state is temporarily unable to handle adequately the return of its nationals, and the state has requested TPS designation; or (3) there exist other extraordinary and temporary conditions in the state that prevent nationals from returning in safety.

TPS beneficiaries are not required to leave the United States and may obtain work authorization for the initial TPS period and for any extensions of the designation. TPS does not automatically lead to permanent resident status. A TPS designation may be effective for a minimum of 6 months and a maximum of 18 months. Before the end of the TPS designation period, the conditions that gave rise to the TPS designation are reviewed. Unless a determination is made that those conditions are no longer met, the TPS designation will be extended for 6, 12, or 18 months. If the conditions that led to the TPS designation are no longer met, the TPS designation is terminated. Designations, extensions, terminations and other documents regarding TPS are published in the **Federal Register**. Currently, nationals of Somalia, Sudan, Burundi, Honduras, Nicaragua, and El Salvador have TPS status in the United States.

In many cases, TPS status for a particular country will remain in place for several years. Thus, nationals of these countries may be in the United States for a decade or more and establish a record that TSA can effectively review for a security threat assessment. Based on this and the unrestricted work authorization, we have determined that under certain circumstances, TPS recipients should be permitted to hold a TWIC. Our ability to complete a thorough threat assessment and the record that is disclosed during the threat assessment will be critical factors in determining if a waiver should be granted to a TPS recipient. In addition, letters of reference from employers, teachers, and religious or spiritual personnel are also important to reach a determination on a waiver. Part 1515 lists the information TSA reviews in making waiver determinations, which now also apply to TPS recipients.

Finally, on October 17, 2006 Congress passed the John Warner National Defense Authorization Act for Fiscal Year 2007 (P.L. 109–364). In that Act, Congress amended 46 U.S.C. 8103 to permit an alien allowed to be employed in the U.S. under the Immigration and Nationality Act who meets additional requirements for service as a steward aboard large passenger vessels to obtain an MMD. Since all MMD holders must obtain a TWIC, we have extended this statutory requirement to TWIC as well. Individuals who would satisfy the statutory requirements would most likely, if not always, possess a C–1/D Crewman Visa. The C–1/D visa has been added to the list of acceptable restricted nonimmigrant visas.

Table 2 indicates the types of visas that a lawful nonimmigrant with a restricted visa must hold in order to demonstrate eligibility to apply for a TWIC.

TABLE 2.—TYPES OF VISAS THAT A NONIMMIGRANT WITH A RESTRICTED VISA MUST HOLD

Visa	Nonimmigrant classifications	Description/information
C–1/D	Combined Transit and Crewman Visa. 8 CFR 214.2(c)(D)	For alien crewmen serving in good faith in a capacity required for normal operation and service on board a vessel who intends to land temporarily and solely in pursuit of his calling as a vessel crewman.
E–1	Treaty Trader (see 8 CFR 214.2(e)(1)).	For nationals of a country with which the United States maintains a treaty of commerce and navigation who is coming to the United States to carry on substantial trade, including trade in services or technology, principally between the United States and the treaty country, or to develop and direct the operations of an enterprise in which the national has invested. The employee must intend to depart the United States upon the expiration or termination of E–1 status.

TABLE 2.—TYPES OF VISAS THAT A NONIMMIGRANT WITH A RESTRICTED VISA MUST HOLD—Continued

Visa	Nonimmigrant classifications	Description/information
E–2	Treaty Investor (see 8 CFR 214.2(e)(2)).	An alien employee of a treaty investor, if otherwise admissible, may be classified as E–2 if the employee is in or is coming to the United States to engage in duties of an executive or supervisory character, or, if employed in a lesser capacity, the employee has special qualifications that make the alien's services essential to the efficient operation of the enterprise. The employee must have the same nationality as the principal alien employer. In addition, the employee must intend to depart the United States upon the expiration or termination of E–2 status.
E–3	Australian in Specialty Occupation.	The E–3 is a new visa category only for Australians coming to the U.S. to work temporarily in a specialty occupation.
H–1B	Specialty Occupations (see 8 CFR 214.2(h)(4)).	Persons who will perform services in a specialty occupation which requires theoretical and practical application of a body of highly specialized knowledge and attainment of a baccalaureate or higher degree or its equivalent (in the specialty) as a minimum requirement for entry into the occupation in the US.
H–1B1	Free Trade Agreement (FTA) Professional Visa (H–1B1).	Foreign nationals of countries which have Free Trade Agreements with the United States and are engaged in a specialty occupation are eligible for the H–1B1 FTA Professional Visa [Free Trade Agreement (FTA) Professional Visa]. A U.S. employer must furnish a job letter specifying the details of the temporary position (including job responsibilities, salary and benefits, duration, description of the employing company, qualifications of the applicant) and confirming the employment offer.
L–1	Executive, managerial	An alien who within the preceding three years has been employed abroad for one continuous year by a qualifying organization may be admitted temporarily to the United States to be employed by a parent, branch, affiliate, or subsidiary of that employer in a managerial or executive capacity, or in a position requiring specialized knowledge.
O–1	Extraordinary Ability or Achievement.	An alien who has extraordinary ability in the sciences, arts, education, or athletics, which has been demonstrated by sustained national or international achievement.
TN	North American Free Trade Agreement (NAFTA) visas for Canadians and Mexicans.	The nonimmigrant NAFTA Professional (TN) visa allows citizens of Canada and Mexico, as NAFTA professionals, to work in the United States.
M–1	Vocational student	This visa category is for a fixed time needed to complete the course of study and training. For purposes of the final rule, only students who are attending the U.S. Merchant Marine Academy or comparable State maritime school and hold this visa are permitted to apply for a TWIC.

We are making an additional change to the application information required of TWIC applicants who are not U.S. nationals. In 49 CFR 1572.17, we are requiring all aliens to bring to enrollment the documents that verify the immigration status they are in as of the date of enrollment. We will examine the documents to ensure that the applicant is eligible to apply for a TWIC under the immigration standards and then scan the documents into the TSA system so that they become part of the enrollment record.

In addition, we are requiring drivers with commercial licenses from Canada to provide a Canadian passport at enrollment, if they do not hold a Free and Secure Trade (FAST) card [6]. We know that Canadian TWIC applicants who hold a FAST card have completed a thorough background check by the Canadian government. However, Canadian provinces do not always require Canadian citizenship or in some cases, lawful presence, when issuing a drivers license. Therefore, we do not believe it is advisable to issue a TWIC based solely on a Canadian driver's license. We are not requiring this of Mexican-licensed drivers who apply for a TWIC because they must obtain border crossing documents to enter the United States, which are issued after the Mexican government has completed a review of the individual and determined they are Mexican citizens or are lawfully present in Mexico.

(e). Mental Incapacity

TSA is changing the waiver process to permit applicants who in the past have been involuntarily committed to a mental health facility or declared mentally incapable of handling their affairs to apply for a waiver without always having to provide documentation showing that the disqualifying condition is no longer present, as we have previously. For example, there may be cases in which an individual has an addiction to drugs or alcohol and is involuntarily committed to a mental health facility to complete rehabilitation. If the individual wishes to apply for a waiver, documents showing that applicant completed rehabilitation successfully would be critical to TSA's determination on the waiver request. The individual may no longer use illegal drugs or drink alcohol, but technically they may still have an addiction. Therefore, we believe TSA should decide these waiver requests on a case-by-case basis. The documentation submitted to TSA in support of the waiver request will be very important in making the waiver determination. Applicants and/or their representatives should carefully consider and include all available information TSA can use to determine if the applicant poses a security threat.

(f). Fees

Section 520 of the 2004 DHS Appropriations Act, Pub. L. 108–90, requires TSA to collect reasonable fees for providing credentialing and background investigations in the field of transportation. Fees may be collected to pay for the costs of: (1) Conducting or obtaining a CHRC; (2) reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; (3) reviewing and adjudicating requests for waivers and appeals of TSA decisions; and (4) other costs related to

[6] The FAST program is a cooperative effort between the Bureau of Customs and Border Patrol (CBP) and the governments of Canada and Mexico to coordinate processes for the clearance of commercial shipments at the U.S.-Canada and U.S.-Mexico borders. Participants in the FAST program, which requires successful completion of a background records check, may receive expedited entrance privileges at the northern and southern borders.

performing the security threat assessment or the background records check, or providing the credential. Section 520 requires that any fee collected must be available only to pay for the costs incurred in providing services in connection with performing the security threat assessment, or the background records check, or providing the credential. The funds generated by the fee do not have a limited period of time in which they must be used. They can be used until they are fully spent. TSA has also established the fees in this final rule pursuant to the requirements of the General User Fee Statute (31 U.S.C. 9701), which requires fees to be fair and based on: (1) Costs to the government; (2) the value of the service or thing to the recipient; (3) public policy or interest served; and (4) other relevant facts.

In this final rule, TSA uses slightly different terminology to describe the three types of fees and their segments than was used in the NPRM. The Standard TWIC Fee is the fee that an applicant would pay to obtain or renew a TWIC. The Standard TWIC Fee contains the following segments:

- Enrollment Segment (referred to as the ''Information Collection/Credential Issuance Fee'' in the NPRM),
- Full Card Production/Security Threat Assessment (STA) Segment (referred to as the ''Threat Assessment/Credential Production Fee'' in the NPRM), and
- FBI Segment (referred to as the ''FBI Fee'' in the NPRM).

The Reduced TWIC Fee is the fee an applicant would pay to obtain a TWIC when the applicant has undergone a comparable threat assessment in connection with an HME, a FAST card, or other threat assessment, as provided in § 1572.5(e), or holds an MMD or License as provided in § 1572.19(b). The Reduced TWIC fee is made up of the following segments:

- Enrollment Segment, and
- Reduced Card Production/STA Segment (referred to as the ''reduced fee for the Security Threat Assessment/Credential Production Fee'' in the NPRM).

The Card Replacement Fee is the fee that an applicant would pay to replace a credential that has been lost, stolen, or damaged and is made up of the Card Replacement Segment.

In the TWIC NPRM, TSA proposed to set the Standard TWIC Fee at $129–149, including the Enrollment Segment of $45–65, the Full Card Production/Security Threat Assessment (STA) Segment of $62, and the FBI Segment of $22. TSA proposed that the Reduced TWIC Fee be set at $95–115, including the Enrollment Segment of $45–65 and the Reduced Card Production/STA Segment of $50.[7] TSA proposed that the Card Replacement Fee, composed of the Card Replacement Segment, be set at $36. *See* 71 FR at 29405, 29428–29431.

In this final rule, TSA establishes the Standard TWIC Fee at $139–159, including the Enrollment Segment of $45–65, the Full Card Production/STA Segment of $72, and the FBI Segment of $22.[8] The total Reduced TWIC Fee is set at $107–127, including the Enrollment Segment of $45–53 and the Reduced Card Production/STA Segment of $62.

In this final rule, TSA establishes the Replacement Card Fee of $36, as was in the NPRM. TSA's analysis shows that this fee is costed out at $60, but is not including that amount in the final rule due to the large difference in amount from the NPRM. TSA proposes in this final rule to change the Replacement Card Fee to $60 based on the reevaluation of costs elements discussed below, and requests comments only on this fee. *See* Request for Comments in Section VI.

Table 3 compares the NPRM per person fee and segments amounts to the final rule per person fee and segments amounts:

TABLE 3.—TWIC PER PERSON FEE SEGMENTS—NPRM VS. FINAL RULE

	NPRM	Final rule	$ Increase	% Increase
Standard TWIC Fee				
Enrollment Segment	$45–$65	$45–$65		
Full Card Production/STA Segment (for Individuals requiring a full STA)	62	72	$10	
FBI Segment:	22	22		
Total	129–149	139–159	10	7.86–6.7
Reduced TWIC Fee				
Enrollment Segment	45–65	45–65		
Reduced Card Production/STA Segment (for Individuals not requiring a full STA):	50	62	12	
Total	95–115	107–127	12	12.6–10.4
Card Replacement Fee				
Card Replacement Segment	36	60[9]	24	66.7

No applicant will be required to pay a fee until after TSA publishes this notice in the **Federal Register**.

Cost Components

The NPRM identified the cost components from which the proposed fees were calculated. These are the same components that were used to calculate the final fees. However, the fees themselves have changed for the reasons described in this section. Since publication of the NPRM, the TWIC program has reevaluated the cost estimates that drive the TWIC fees. Table 4 lists the cost components of the TWIC Program as estimated for the NPRM and compares them to the costs estimated for the final rule. These cost components are used to derive the TWIC fees that must be collected to fully recover program costs.

[7] While the proposed rule text at § 1572.503(2) indicated that the Reduced TWIC Fee included both the Enrollment Segment and the Reduced Card Production/STA Segment, it erroneously listed the fee at $50. The total for this fee was correctly stated in the preamble as $95. See 98 FR at 29045.

[8] If the FBI changes its fee in the future, TSA will collect the amended fee.

[9] While this rule sets a Card Replacement Fee of $36, TSA is proposing that the Card Replacement Fee be increased to $60 and is seeking comment only on the Card Replacement Fee. See Request for Comments Section VI.

TABLE 4.—5-YEAR TOTAL TWIC COST COMPONENTS—NPRM VS. FINAL RULE

Cost components	NPRM	Final rule	Percent change	Standard TWIC fee	Reduced TWIC fee	Card replacement fee
Enrollment/Issuance	$65,212,285	$65,980,199	1	X	X	X[10]
Threat Assessments[11]	42,463,118	32,120,927	−24	X	X[12]	.....
IDMS	18,783,000	44,190,882	135	X	X	X
Card Production	20,427,000	28,346,657	39	X	X	X
Program Support	22,641,000	18,810,786	−17	X	X	X
Total	169,526,403	189,449,451	12			

As shown by Table 4, some of the cost components decreased from the NPRM costs estimates, while some increased. The Enrollment/Issuance cost component increased by approximately 1 percent due to further analysis that indicated a need to account for the contractor fee associated with replacing a lost, stolen, or damaged card. This contractor fee is estimated at $5. This card re-issuance cost within the Card Replacement Fee was not included as part of the NPRM estimate.

The Threat Assessments cost component decreased overall by approximately 24 percent. While the costs associated with adjudication by ALJs have been added, cost reductions for perpetual vetting and threat assessment gateway account for the overall reduction.

The IDMS cost component increased based on a re-evaluation of the overall IDMS costs. The program office identified: (1) The need to increase the hardware and software required to obtain a Security Certification & Accreditation, and to support the full volume of TWIC applicants; (2) system changes required to address security vulnerabilities; and (3) increases in contractor support necessary for systems operations and maintenance. The total increase is estimated at $19 per credential produced.

The Card Production cost increased by approximately 39 percent based on two factors. First, in order to produce cards more rapidly during the initial enrollment, additional shifts were required at the card production facility. This decision was made in order to address comments to the NPRM that cards needed to be produced as quickly as possible. Second, TSA and Coast Guard received comments to the NPRM on the need to support contactless biometric authentication based on the harsh conditions of the maritime environment and operational efficiencies. In order to address these comments TSA and the Coast Guard have established a NMSAC working group to recommend a contactless TWIC technology specification. Second, we have added a fee to cover future technology-related product improvements to the TWIC system and credential. Technology improvements occur rapidly and in order to take advantage of the efficiency these improvements provide, we must plan for that cost. Building in the cost of technology and system improvements is a common practice for programs that rely so heavily on software and hardware to collect and transmit large amounts of information.

The Program Support cost decreased by approximately 17 percent because the program office reevaluated and decreased program staffing levels required to support the maritime population after the initial maritime enrollment period. Additionally, Program Support costs related to interagency communication requirements also decreased. These cost reductions resulted in approximately a $2 per card decrease.

The discussion below describes the cost components associated with each type of fee, Standard, Reduced and Card Replacement. Although the overall program costs increased by approximately 12 percent, the three types of TWIC fees did not increase by 12 percent as each fee is composed of different cost components.

The per person cost segments for the Standard TWIC Fee are derived from all five of the cost components in the Total TWIC Cost Components table above—Enrollment/Issuance, Threat Assessments,[13] IDMS, Card Production, and Program Support. Note that the IDMS, Card Production, Program Support cost components makeup the Card Production/STA and FBI segments of the Standard and Reduced TWIC Fees. The net increase in the total for the Standard TWIC Fee is based primarily on the increase of the IDMS and Card Production cost components, as described above in the analysis of the TWIC cost components.

The per person cost segments for the Reduced TWIC Fee are also derived from five of the cost components in the Total TWIC Cost Components Table 4—Enrollment/Issuance, Threat Assessments,[14] IDMS, Card Production, and Program Support. The net increase in the Reduced TWIC Fee is based on the reevaluation of the cost components, as described in the analysis of the TWIC cost components above. It should be noted that the reduced fee does not include the entire Threat Assessments cost component. Because the Reduced TWIC Fee does not include this entire cost component, this fee does not entirely benefit from the reduction in the Threat Assessments cost component, and therefore, increased at a greater percentage than the Standard TWIC Fee.

The per person cost for the Card Replacement Fee is derived from four of the cost components in the Total TWIC Cost Components Table 4—Enrollment/Issuance,[15] IDMS, Card Production, and Program Support. The net increase in the Card Replacement Fee of $24 is based on the reevaluation of the cost components, as described in the analysis of TWIC cost components

[10] While the majority of the Enrollment/Issuance requirements have already been satisfied by the applicant through initial enrollment, there are still some enrollment/issuance functions associated with these card replacements, such as overhead. Therefore, these applicants will not be burdened with the normal enrollment/issuance cost component.

[11] The Threat Assessments, IDMS, Card Production and Program Support Components makeup the Card Production/STA and the FBI Segments.

[12] While the majority of the Threat Assessment requirements have already been satisfied by the applicant through participation in a previous security fee, there are still some threat assessment functions associated with these applicants, such as CSOC activities. Therefore, these applicants will pay the Reduced Card Productions/STA Segment.

[13] The Threat Assessment cost component includes the FBI Segment of the Standard TWIC Fee.

[14] As stated in footnote 11, although the majority of the Threat Assessment requirements have already been satisfied by the applicant through participation in a previous security fee, there are still some threat assessement functions associated with these applicants.

[15] As stated in footnote 10, although the majority of the Enrollment/Issuance requirements have alread been satisfied by the applicant through initial enrollment, there are still some enrollment/issuance functions associated with these card replacements, such as overhead.

above. It should be noted that this fee does not include the entire Enrollment/Issuance cost component or any of the Threat Assessments cost component. Because this fee does not include the Threat Assessments cost component, this fee does not benefit from the reduction in the Threat Assessments cost component. Thus, the Card Replacement Fee has increased at a greater percentage than the Standard and Reduced TWIC Fees. Because this fee is substantially higher than that in the NPRM, TSA is establishing $36 as the fee in this rule but is proposing to increase the fee to $60 and is providing the public an opportunity to submit additional comments on the card replacement fee. *See* Request for Comments in Section VI.

An Additional Notice on Fees

As Table 3 indicates, the Enrollment Segment is a range of $45–$65 for both the NPRM and the final rule. TSA is unable to finalize the fee because we do not yet have a final contract with an enrollment provider. When a final contract is executed, TSA will publish a Notice in the **Federal Register** that will specify the amount for that segment and all of the fees. Therefore, the rule text does not contain TSA's exact fee numbers, but it does include the FBI fee. No applicant will be required to pay a fee until after TSA publishes this notice in the **Federal Register**.

(g). Drivers Licensed in Mexico and Canada Transporting Hazardous Materials

In accordance with sec. 7105 of SAFETEA–LU, commercial motor vehicle drivers licensed in Canada or Mexico may not transport hazardous materials into or within the United States unless they undergo a background check that is similar to that undergone by U.S.-licensed drivers.[16] TSA has determined that a card issued by the Bureau of Customs and Border Protection (CBP) under the FAST program provides a similar background check. *See* 71 FR 44874 (August 7, 2006). The security threat assessment that is required under this final rule for issuance of a TWIC is the same background check currently required for U.S.-licensed drivers with HMEs. Therefore, we are amending 49 CFR 1572.201 to allow possession of a TWIC card by a driver licensed in Mexico or Canada to satisfy the SAFETEA–LU requirement. Thus, drivers licensed in Canada or Mexico may obtain either a FAST card or a TWIC to meet the requirement that they have a background check that is similar to that of a U.S. hazmat driver.

In this final rule, for administrative purposes, we are reprinting the entire part 1572. We are making only a couple of changes to § 1572.203, however. We are changing its title to more clearly reflect its scope, to ''Transportation of explosives from Canada to the United States via railroad carrier.'' In § 1572.203(b) we are changing the definition of ''Customs Service'' to ''Customs and Border Protection (CBP)'' to reflect the reorganization of the U.S. Customs Service under the Homeland Security Act of 2002.

(h). Compliance and Enforcement Matters

We are adding a new section. (49 CFR 1570.7) to make it clear that it is a violation of this rule, and other applicable federal laws, to circumvent or tamper with the access control procedures. This section also clarifies that it is a violation for any person to use or attempt to use a credential that was issued to, or a security threat assessment conducted for, another person. In addition, no person may make, cause to be made, use, or cause to use, a false or fraudulently-created TWIC or security threat assessment issued or conducted under this subchapter. Finally, it is a violation of this rule, and other applicable federal laws, for any person to cause or attempt to cause another person to violate these procedures. Violations of any provision of this rule may be subject to such civil, criminal or administrative actions as are authorized under federal law.

Note that the acts identified in § 1570.7 may also be violations of Federal criminal law, such as 18 U.S.C. 701 (Official badges, identification cards, other insignia), 18 U.S.C. 1001 (Statements or entries generally), 18 U.S.C. 1028 (Fraud and related activity in connection with identification documents and information), 18 U.S.C. 1029 (Fraud and related activity in connection with access devices). In appropriate cases, TSA will refer to the Department of Justice (DOJ) matters for criminal investigation and, if appropriate, criminal prosecution.

Section 1570.9 is being added to make clear that a person must allow his or her TWIC to be inspected upon request of an appropriate official. For clarification purposes, Coast Guard has provided a similar requirement in 33 CFR 101.515(d) adopting the same language as § 1570.9.

As discussed in section C.4. of this preamble, § 1570.11, Compliance, inspection, and enforcement, was proposed in the NPRM as § 1572.41.

D. Anticipated Future Notices and Rulemaking

1. Notices

We will publish several notices in the **Federal Register** to facilitate implementation of the TWIC program. Specifically, a notice will be published:

(a) establishing the fees for the TWIC, as stated above in C.2(f);

(b) for each COTP zone, prior to beginning the enrollment period; and

(c) for each COTP zone, 90-days prior to requiring compliance with these regulations.

2. Rulemaking

In the future we will issue another NPRM to propose card reader requirements for MTSA-regulated vessels and facilities. It will be issued with a comment period that is long enough for all interested persons to reasonably be able to provide comment, and it will announce public meetings in a variety of places. We cannot, at this time, make any definitive statement on where those places will be, but we will consider the locations suggested by commenters and inform the public of upcoming meeting information in advance in the **Federal Register**.

E. Summary of TWIC Process Under the Final Rule

The TWIC program was developed to improve identity management and credentialing shortcomings that exist in segments of the transportation industry. TSA evaluated a variety of technologies, used field testing, and to the extent possible, incorporated the basic tenets of Homeland Security Presidential Directive 12 (HSPD–12) [17] to arrive at the credential and enrollment process implemented in this program. The standards for the program are to ensure that the credentialing processes: (1) Are administered by accredited providers; (2) are based on sound criteria for verifying an individual's identity; (3) include a credential that is resistant to fraud, tampering, counterfeiting and terrorist exploitation; and (4) ensure that the credential can be quickly and electronically authenticated.

The purpose of the TWIC program is to ensure that only authorized personnel who have successfully completed a security threat assessment have unescorted access to secure areas of maritime facilities and vessels. The credential will include a reference biometric that securely links the credential holder to the issued

[16] 49 U.S.C. 5103a(h).

[17] HSPD–12 requires Federal agencies and their contractors to adopt an identity management and credentialing system that uses biometrics.

credential. At any time, TWIC holders may be asked to confirm that they are the rightful owner of the credential by matching their biometric to the one stored on the credential. An individual's credential is revoked by TSA if disqualifying information is discovered or the credential is lost, damaged or stolen. When a credential is revoked, TSA lists it on the list of revoked cards, or 'hotlist' by the unique serial number assigned to the credential. Therefore, a revoked credential that is compared against the hotlist will be flagged and access would not be granted.

TSA has designed the TWIC process to maintain strict privacy controls so that a holder's biographic and biometric information cannot be compromised. The TWIC process implemented in this rule is described below from the perspective of an applicant.

1. Pre-Enrollment and Enrollment

TWIC enrollment will be conducted by TSA or TSA's agent operating under TSA's direction. These personnel are known as Trusted Agents. All Trusted Agents must successfully complete a TSA security threat assessment and receive extensive training before they are authorized to access documents, systems, or secure areas.

DHS will publish a notice in the **Federal Register** indicating when enrollment at a specific location will begin and when it is expected to terminate. Once DHS has published that notice, facility and vessel owners/operators (owners/operators) must notify workers of their responsibility to enroll into the TWIC program during the enrollment period. Regarding the compliance date for facilities, DHS will also publish this information in the **Federal Register** for each COTP zone at least 90-days in advance. Owners and operators are required to inform their employees of this date as well. (The implementation plan for enrollment is discussed in greater detail below.) TSA and the Coast Guard will work with owners/operators to ensure that they can provide applicants sufficient time to enroll, complete the security threat assessment and any necessary appeal or waiver process, and obtain the credential before the applicant is required to present the credential for access to a facility or vessel. As TWIC is implemented, owners/operators must give individuals at least 60 days notice to begin the enrollment process. Generally, TSA completes a threat assessment in approximately 10 days when there is no indication that the applicant may not meet the TWIC enrollment criteria. If criminal activity or other potentially disqualifying information is revealed, however, TSA cannot guarantee that such information will be favorably resolved and a threat assessment completed in less than 30 days.

Applicants are encouraged to ''pre-enroll'' online to reduce the time needed to complete the entire enrollment process at an enrollment center. The convenience of pre-enrollment is a significant benefit for applicants and reduces strain on the enrollment centers. The pre-enrollment process allows applicants to provide much of the biographic information required for enrollment and to select an enrollment center where they wish to complete enrollment. While pre-enrolling, applicants may schedule an appointment to complete enrollment at an enrollment center, although appointments are not required at enrollment centers. For pre-enrollment, applicants may use a personal computer with access to the internet or they may use TWIC kiosks. The TWIC kiosks will be set up by the TSA agent when enrollment begins at locations convenient to the affected population, including enrollment centers, and are similar to an ATM machine.

The Web address for pre-enrollment and all additional information relating to the TWIC program is *www.tsa.gov/twic.* The TWIC Web site also will list the documents the applicant must bring to the enrollment center to verify identity so that all applicants can be properly prepared. Mariners who must prove U.S. citizenship or immigration status to obtain an MMD, license, COR, STCW endorsement or MMC must provide the documents required by the Coast Guard at 46 CFR chapter I, subchapter B at the time of enrollment.[18] TSA will scan these documents into the enrollment record, which will be forwarded to the Coast Guard. In addition, applicants who are not U.S. citizens or nationals must bring their immigration documents, including visas and naturalization paperwork, to enrollment so that the documents which prove legal presence in the United States can be scanned into the enrollment record.

At the enrollment center, applicants who pre-enroll must provide documents to verify their identity, confirm that the information provided during pre-enrollment is correct, submit biometrics identifiers, and sign the enrollment documents. At the enrollment center, all applicants will receive a privacy notice and consent form, by which they agree to provide personal information for the security threat assessment and credential. (For applicants who pre-enroll, the privacy notice is provided with the application on-line, but the applicant 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 consent form and identity documents, is scanned into the TSA system for storage. All information is encrypted or stored using methods that protect the information from unauthorized retrieval or use. If an enrollment center temporarily loses its internet connection, the enrollment data is encrypted and stored on the enrollment workstation, but only until an internet connection is restored.

Applicants will provide fingerprints from each hand and sit for a digital photograph. We will collect a print from all 10 fingers unless the applicant has lost or seriously injured his or her fingers. TSA will provide alternative procedures for enrollment centers to use if an applicant cannot provide any fingerprints. The fingerprints and photograph will be electronically captured at the enrollment center and made part of the applicant's TWIC enrollment record. The fingerprint images collected from each applicant will be submitted to the FBI for the CHRC.

The TWIC fee, which covers the cost of enrollment, threat assessment, and credential production and delivery, will be collected from the applicant at the enrollment center. Payment can be made by cashier's check, money order, or credit card. The TWIC enrollment fee is non-refundable, even if the threat assessment results in denying a TWIC to the applicant.

The entire enrollment record (including all fingerprints collected) will be transmitted to the TSA system, encrypted, and segmented to prevent unauthorized use. The TSA system acknowledges receipt of the enrollment record, at which time all enrollment data is automatically deleted from the enrollment workstation. At this point,

[18] In order to allow the Coast Guard to remove the requirement that all mariners apply for their credentials in person at a Regional Examination Center (REC), it is necessary for TSA to document proof of citizenship, as the citizenship requirements for certain Coast Guard-issued mariner credentials are stricter than the overall TWIC citizenship requirements. For more information on mariner credentials and the Coast Guard's plan to remove the physical appearance at an REC requirement, *see* the Coast Guard SNPRM titled ''Consolidation of Merchant Mariner Qualification Credentials'' published elsewhere in today's **Federal Register**.

enrollment data is stored only in the TSA system, and is stored there as encrypted data. The TSA system contains many feedback mechanisms to validate the transmission and receipt of data at key points in the process. The status of each transmission is recorded within the system.

As discussed in the TWIC NPRM (71 FR 29402), during TSA's Prototype testing phase of the program, the average time needed for an applicant who pre-enrolled to complete enrollment was 10 minutes, 21 seconds. TSA expects that it will take approximately fifteen minutes to complete enrollment of applicants who do not pre-enroll.

TSA and Coast Guard plan to use a phased enrollment approach based on risk assessment and cost/benefit analysis to implement the program nationwide. Locations that are considered critical and provide the greatest number of individual applicants will be among the earliest enrollment sites. As stated above, TSA will publish a notice in the **Federal Register** indicating when enrollment at a specific location will begin and when it is expected to terminate. In addition, DHS will publish a notice in the **Federal Register** indicating the compliance date for each COTP zone. This notice will be published at least 90 days prior to the compliance date. There are approximately 130 locations where TSA plans to enroll applicants. TSA and Coast Guard will work closely with the maritime industry to ensure that owners/operators and workers are given as much notice as possible of the commencement of enrollment at their location. (See the discussion of § 1572.19 below for additional information on the timing of enrollment.) TSA will use a combination of fixed and mobile enrollment stations to make the enrollment process as efficient as possible for applicants and owners/operators.

2. Adjudication of Security Threat Assessment

Following enrollment, the TSA system sends pertinent parts of the record to various sources so that appropriate terrorist threat, criminal history, and immigration checks can be performed. When the checks are completed, TSA makes a determination whether to issue a TWIC to the applicant and notifies the applicant of that decision. If the applicant is deemed to be qualified, the TSA system notifies the credential production portion of the system to create a credential. TSA sends the applicant a Determination of No Security Threat via U.S. mail, and the TSA system notifies the applicant when the credential is ready to be retrieved from the enrollment center. Notifications from the TSA system that a credential is ready for pick-up will be through e-mail or voice mail, depending on the preference the applicant expresses on the application.

If TSA determines that the applicant is not qualified, TSA sends an Initial Determination of Threat Assessment to the applicant via U.S. mail, with information concerning the nature of the disqualification, and how the applicant may appeal the determination or apply for a waiver of the standards. If the applicant proceeds with an appeal or application for waiver that is successful, TSA will notify the applicant accordingly and the credential production process begins. (The appeal and waiver processes are discussed in greater detail below in the discussion of 49 CFR part 1515.)

3. Credential Production and Delivery

If the applicant is deemed by TSA to be qualified to receive a TWIC, the TSA system generates an order to produce a credential. The TWIC is produced at a government credential production facility. The face of the TWIC credential contains the applicant's photograph, name, TWIC expiration date, and a unique credential number. In addition, the credential will store a reference biometric, a personal identification number (PIN) selected by the applicant, a digital facial image, an expiration date, and a Federal Agency Smart Credential number. The PIN can subsequently be used as an additional security factor in authenticating identity and authorizing use of the credential; or it can be used as the primary verification tool if the biometric is inoperative for some reason.

4. Receiving the Credential

The TSA system will notify the applicant when the credential is ready, and what if any additional steps the applicant must take to receive the credential. Once the enrollment and issuance process is completed, the credential is activated and is ready to be presented at a facility or vessel for use as an access control tool. The TWIC security threat assessment and credential are valid for five years, unless information is discovered that causes TSA to revoke the credential.

5. Lost, Damaged, or Stolen TWICs

Replacement TWICs are available if a credential is lost, stolen, or damaged. As soon as a TWIC holder becomes aware that his credential is missing or damaged, he must report this fact by calling the TWIC Call Center which will be open 24 hours per day, 7 days a week. TSA will post the Call Center number on the TWIC web site as soon as it is available, and it will be posted at all enrollment centers and kiosks. The Center follows a standard process to revoke the credential, and order printing and transmission of a replacement. TSA adds the lost, damaged or stolen credential to the 'hotlist,' which includes the Smart Card number of all credentials that TSA has revoked. Applicants must pay a fee of $36[19] to cover the cost of invalidating the previous credential, production of a replacement credential, shipping, and other appropriate program costs. The reissued TWIC will have the same expiration date as the lost/damaged/stolen TWIC.

6. Renewal

TWICs issued under this rule remain valid for a period of five years, unless renewed before the five-year term ends. Upon renewal, an applicant receives a new credential and the old credential is invalidated in the TSA System. TSA does not plan to notify TWIC holders when their credential is about to expire because the expiration date will be displayed on the face of the credential. To renew a TWIC, the holder must appear at any enrollment center, at least 30 days before expiration, to initiate the renewal process. This will provide sufficient time for TSA to conduct the security threat assessment and the Coast Guard to complete any review necessary to renew any required mariner documents. During renewal, applicants must provide the same biographic and biometric information and identity verification documents required in the initial enrollment and pay the associated fees. Note that the TWIC web site will maintain a list of documents that may be used to verify identity, which may change over time. A new credential is issued upon renewal using the same issuance process as used in the initial TWIC issuance and the expired credential will be invalidated. The newly issued credential will have an expiration date five years from the date of issuance of the new credential. Although renewal only occurs every five years, TSA conducts recurring checks on individuals throughout the five year period, so that newly-discovered information informs the access rights of individuals.

[19] We request comments on changes to the card replacement fee in Section VI below.

7. Call Center

Toll-free TWIC Call Center (Help Desk) support will provide around-the-clock service for transportation workers, facility operators, and others who require assistance. Assistance includes help for pre-enrollment; enrollment; and lost, stolen, or damaged card reporting and replacement. Help will also be available for scheduling enrollment appointments, locating the closest enrollment facility to an applicant, guiding applicants through the Web-based pre-enrollment process, and for checking on the status of a TWIC application.

F. SAFE Port Act of 2006

On October 13, 2006, the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Pub. L. 109–347) was enacted. The portions of the Act which relate to the TWIC program are discussed below.

Section 104(a) of the SAFE Port Act contains a number of amendments to the basic requirement in MTSA for credentialing codified in 46 U.S.C. 70105. New sec. 70105(g) mandates concurrent processing by TSA and the Coast Guard of an individual's application for an MMD [20] and a TWIC. This final rule is in compliance with this requirement. TSA will share with the Coast Guard the individual's CHRC, fingerprints, photograph and proofs of citizenship and identity, which will allow the Coast Guard to begin evaluating whether the individual is qualified to obtain an MMD while TSA completes its security threat assessment. TSA will also share the results of their security threat assessment with the Coast Guard to ensure that MMDs are only issued to individuals who pass the security threat assessment and are issued a TWIC. Thus, such applicants will only submit one set of fingerprints and other information relating to citizenship, alien status, and criminal history, which will be used by both TSA and the Coast Guard.

New sec. 70105(h) requires that applicants who have passed a security threat assessment for an HME or MMD pay only for the costs associated with the issuance, production, and management of the TWIC and are not charged for the cost of another threat assessment. This final rule is in compliance with this requirement in that TSA will not charge those who already hold an HME or MMD for an additional threat assessment under TWIC. Rather, TSA will charge a reduced fee.

New sec. 70105(i) provides requirements for implementing TWIC across the nation by prioritizing the ports based on risk, and requires that the TWIC program is to be implemented according to the following schedule: (1) top ten priority ports by July 1, 2007; (2) the next forty priority ports by January 1, 2008; and (3) all other ports by January 1, 2009. Under new sec. 70105(j) each application for a TWIC made by someone holding an MMD as of the date of enactment of this bill must be processed by January 1, 2009. We are now planning how to meet these requirements and will establish the implementation schedule accordingly.

New sec. 70105(k) requires DHS to conduct a pilot program on card readers as set out in that section. DHS is currently analyzing how best to meet these requirements, and will begin the pilot program as soon as practicable.

Under new sec. 70105(m) DHS may not require card readers to be placed aboard a ship unless the crew's number is in excess of the number determined to require a reader or if the Secretary determines that the vessel is at risk of a severe transportation security incident. When DHS drafts the rule that will require use of card readers by vessel owners and operators, it will do so in compliance with this requirement.

SAFE Port Act sec. 104(b) has additional amendments to MTSA. It revises 46 U.S.C. 70105(b) by adding a paragraph making clear the Secretary has the discretion to add to the list of those individuals who otherwise may be required to obtain a TWIC. The Secretary may apply TWIC requirements to individuals including those ''not otherwise covered by this subsection''. TSA has exercised this discretion by allowing Canadian and Mexican commercial drivers who transport hazardous materials to obtain TWICs, which will allow them to transport hazardous materials in the United States. Further, SAFE Port Act sec. 104(b) clarifies in sec. 70105(c) that DHS must establish a waiver and appeal process for applicants denied a TWIC under sec. 70105(c)(1)(A) or (B) (criminal history) or (D) (otherwise poses a security threat). TSA's new process in 49 CFR part 1515 complies with this requirement.

Under SAFE Port Act sec. 104(c), the deadline for final TWIC regulations remains January 1, 2007. Further, the regulation must include a provision for an interim check against terrorist watchlist databases so as to enable new workers to start working immediately. This final rule is in compliance with this requirement. As explained in detail elsewhere in this preamble, owners or operators wishing to put their newly hired direct employees to work immediately, prior to issuance of the new hire's TWIC, may do so provided that the new hire is successfully checked against various terrorist databases. The procedure for running the new hire's information through these checks can be found in 33 CFR 104.267, 105.257, and 106.262.

SAFE Port Act sec. 106 states that applicants convicted of treason, espionage, sedition, and crimes listed in chapter 113B of title 18, U.S.C., or comparable State laws must be disqualified from holding a TWIC. The list of disqualifying crimes in 49 CFR 1572.103 complies with this requirement by including these crimes as disqualifying.

III. Discussion of Comments

TSA and the Coast Guard received approximately 1770 comments on the TWIC NPRM during the 45-day comment period. In addition, an estimated 1200 people attended the four public meetings that were held between May 31 and June 7, 2006. Copies of the written comments received, as well as transcripts of the public meetings, are available to the public on *www.regulations.gov* at the public docket for this rulemaking action.

Numerous commenters supported the concept and purpose of the TWIC program as a method of protecting national maritime security. Some expressed their support unequivocally. One commenter requested that its port be selected for the first phase of the enrollment and implementation process. Several commenters who generally agreed with the idea of the TWIC, also criticized certain details of the proposal, expressed qualifications of various kinds, or said the proposal needed to be more efficient, workable, and fair. Some terminal operators and marine engineers who supported TWIC said that although it would achieve greater maritime security, they were concerned about its burden on industry or noted that security needed to be balanced against fairness for maritime workers. One commenter who generally supported the implementation of TWIC was concerned about the impact of the proposed rules on the efficiency of port facility operations, and suggested a more phased and flexible approach. Another commenter asked for more of a risk-management approach with a performance-based set of guidelines and a reevaluated technology. An

[20] Although the SAFE Port Act only created this requirement for MMDs, TSA and the Coast Guard have also applied concurrent processing, a longer time period to apply for an initial TWIC, and reduced fees to licenses, CORs, STCW endorsements, and the MMC.

association of maritime operators supported security and background checks and digital fingerprint and photographs, but was concerned about the short timeline for implementation, the absence of facilities to provide the necessary services, and the social and economic burden imposed on individuals. Another commenter who supported TWIC thought that the requirements for who must possess a TWIC was over inclusive and that waivers or exemption processes should be added to lower the overall number of people who would require a TWIC. A commenter noted that although employers were responsible for notifying employees of the TWIC requirement, employer sponsorship of the TWIC program was not desirable.

In contrast, many commenters expressed strong general opposition to TWIC without providing explicit reasons. Some said it was unnecessary and unjustified, and would not improve maritime security. Some argued that the rule would be harmful. These commenters cited concerns that TWIC was not the most effective and economic approach, it would adversely affect staffing of vessels and port facilities, and it would cause economic hardship on the industry and individuals. Commenters also stated that TWIC was inappropriate for the inland marine industry, it would harm stevedore/terminal operators, and it was an unnecessary cost and duplication of effort where seaport access credentials are currently in use. One commenter stated that although the current system of licensing and documenting maritime personnel is failing or broken, the addition of TWIC will only add additional delays and burden. One commenter argued that the largest threat existed from foreign vessels, and they should not be excluded. Another commenter found the rule ''large-port-centric'' and disapproved of this ''one-size-fits-all'' approach.

TSA's and Coast Guard's responses to the comments are discussed below.

A. Requests for Extension of Comment Period and Additional Public Meetings

We received numerous requests to extend the comment period past the 45 days provided in the NPRM. We also received a significant number of comments requesting that we hold additional public meetings. These requests included a large number of supporting reasons.

Several commenters said that TSA and the Coast Guard had not done enough to obtain information about the concerns of affected maritime workers and industries before going forward with the TWIC rule, and the rule schedule should be extended to allow time for the collection of more information, with public meetings in more sections of the country, such as the Gulf Coast and Great Lakes ports. One commenter said the rule was skewed toward the issues involving large ports. A U.S. Senator argued that more information should have been collected on the impact of the rule on both the inland barge industry and the for-hire passenger excursion boat industry, and an association argued that there was little appreciation of the operational realities of the tugboat, towboat, and barge industry. Another commenter saw little reference to the domestic passenger fleet. Commenters listed the following organizations that they thought should have been consulted: the Passenger Vessel Association, American Waterways Operators Association, the Towing Safety Advisory Committee, the Merchant Personnel Advisory Committee, American Petroleum Institute (API), Offshore Mariner Safety Association (OMSA), and other maritime organizations.

We have carefully considered the comments submitted and nonetheless determined that it is not advisable to extend the comment period, nor did we hold additional public meetings. We considered delaying implementation of this entire project but determined that the security risk associated with such a delay is not acceptable. While the ''name checks'' being completed by TSA under the Notice published by the Coast Guard on April 28, 2006 (71 FR 25066) do provide some security to the ports, we need the added layer of security that issuing TWICs provides. First, the current name check regime established through the Coast Guard Notice checks names against the terrorist watch lists and immigration databases. With TWIC, we will also check an individual's criminal history and conduct an enhanced immigration check. Second, the interim vetting regime only applies to permanent employees and long-term contractors of facilities and longshoremen, whereas the TWIC program provides the benefit of performing checks on all individuals with unescorted access to both facilities and vessels. Finally, the TWIC program will provide the owners/operators with the piece that the interim vetting regime is missing—namely, a universal credential to verify whether an individual requesting access to a vessel or facility has been screened and determined not to be a security threat. With the Coast Guard spot checks, we can also verify, on a random basis, the validity of the TWICs being used to gain entry to vessels and facilities.

As we began reviewing the comments we received at the public meetings and on the docket, we realized that there were some portions of the NPRM that were not ready to be implemented. Most important among these pieces were the card reader and biometric verification requirements. As a result, we have removed those requirements from the final rule. What remains is the requirement to apply for and hold a TWIC, the threat assessment standards to be used when processing TWIC applications, and the reduced access control requirements, where the TWIC is used as a visual identity badge at MTSA-regulated vessels and facilities. The Coast Guard intends to integrate the TWIC requirements into its already existing facility and vessel annual MTSA compliance exams, as well as through unannounced security spot checks to confirm the identity of the TWIC holder using hand-held card readers.

We will initiate a new rulemaking action after pilot testing TWIC readers in the maritime environment. Through that rulemaking action we will propose, seek comment on, and finalize the requirements for card readers. We will also hold public meetings during that rulemaking action, and will consider holding these meetings in any location suggested by commenters. Thus, while we determined that it was not in the public interest to delay implementation of the TWIC program to allow for an extended comment period or additional public meetings, we will be providing an additional opportunity for public participation before owners/operators of vessels and facilities will have to implement the card reader requirements.

B. Coast Guard Provisions

1. Definitions

(a) Requests To Add Additional Definitions

One commenter felt that using the word ''ensure'' in the regulations establishes an unreasonable standard of care that would require facilities to guarantee safety, and expose facilities to strict liability in the case of a terrorist incident. The commenter recommended that the final rule amend all uses of the word ''ensure'' in 33 CFR, chapter I, subchapter H.

We disagree. The word ensure, as used in current regulations as well as the TWIC NPRM, was used throughout subchapter H purposely, to designate where the ultimate responsibility for

various security functions would be found for enforcement purposes. We did not propose changing it in the TWIC NPRM and we have not changed it in the final rule.

One commenter recommended that the final rule better define the term ''Federal Official'' in 33 CFR 101.514, so that active duty and reserve military personnel, all Federal Civil Service employees, and people who hold Department of Defense (DOD) Common Access Card (CAC) cards are not required to obtain or possess a TWIC. We disagree with the suggested change, as the term Federal official is clear enough on its face, meaning individuals who are working for the Federal government. Section 101.514 allows these individuals to gain unescorted access to a vessel or facility using their agency-issued, HSPD–12 compliant identification card. Until an HSPD–12 card is available, these officials may use their agency's official credential—when representing that agency on offical duty—if that is the DOD CAC card, then the CAC card may be used.

One commenter noted that a definition for the term ''official'' is not provided in the proposed rule, and recommended that Federal, State, and local ''officials'' not requiring a TWIC for unescorted access should be limited to law enforcement, fire, rescue, and government employees that have been subjected to a background screening equivalent to the one conducted for issuance of a TWIC. We believe that the term ''official'' is clear enough in context, and as such we have not added a definition as suggested by the commenter. We recognize, however, that emergency responders may not fit into the ''officials'' category, and so we have added a new paragraph to § 101.514 to cover emergency responders during emergency situations.

One commenter recommended that the rule be amended to exclude persons working on vessels whose sole purpose is entertainment, such as musicians on passenger vessels. If this exclusion was not made, the commenter recommended that where a vessel engaged solely in entertainment has been inadvertently grouped with vessels of other classes, that the designation of various spaces aboard the vessels, and within those vessels' facilities, be more clearly defined in the final rule, including: (1) For passenger vessels, exclude the employees, whose workstation is limited to areas accessible by passengers, based on the fact that they are occupying the same areas as the passengers who are not subject to the requirement; and (2) apply the TWIC ruling only to the crew areas or persons with access to crew areas. This would allow operators to maintain the security of control stations, equipment rooms and voids, without disruption of access to other employee only areas of the vessel or a facility, which do not need to be restricted areas.

We agree with this comment. As discussed above in the section discussing changes to the Coast Guard provisions, we are adding a definition for ''employee access areas,'' for use only by passenger vessels and ferries. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the VSP. Note, however, that any employee that needs to have unescorted access to areas of the vessel outside of the passenger or employee access areas will need to obtain a TWIC.

(b). TWIC

Two commenters recommended that all references to a ''valid TWIC'' be changed to ''TWIC'' since the definition of TWIC requires that it be valid and non-revoked. We agree and have made the suggested changes within 33 CFR parts 101 through 106. We have left the language in 46 CFR parts 10, 12, and 15, however, because in those places, the term TWIC is not tied to the definition in § 101.105.

(c). Public Access Area/Passenger Access Area

One commenter recommended that the definition of ''public access area'' for cargo vessels be the same as that for passenger vessels to allow similar flexibility. Alternatively, the commenter provided a separate definition of ''public access area'' that allows facilities to designate any area as such, provided the area is specified in the FSP.

One association noted that vessels other than ''passenger vessels'' are permitted to carry passengers, industrial personnel, or persons in addition to the crew. The association recommended that the final rule provide flexibility similar to passenger vessels for other types of vessels by providing the following definition of public access areas in 33 CFR part 101: ''Public access areas means those defined spaces within a vessel, facility or OCS facility that do not require a TWIC for unescorted access. Any vessel, facility or OCS facility may designate areas as public access areas provided they are specified in the security plan.''

They further recommended that facilities owners and operators be provided flexibility similar to that of passengers in designating public access areas, and recommended that the following definition be added to part 105:

''§ 105.xxx Public access area.

(a) Any facility may designate areas within the facility as public access areas. Any such areas must be specified in the FSP.

(b) Public access areas are those defined spaces within a facility that do not require escorted access for persons not in possession of a TWIC.''

They also recommended that OCS facilities owners and operators be provided flexibility similar to that of passenger vessels in designating public access areas, and recommended that the following definition be added to part 106:

''§ 106.xxx Public access area.

(a) Any OCS facility may designate areas within the facility as public access areas. Any such areas must be specified in the FSP.

(b) Public access areas are those defined spaces within an OCS facility that do not require escorted access for persons not in possession of a TWIC.''

We disagree with these comments. The concept of a ''passenger access area'' has been included in the final rule to cover passenger vessels, ferries, and cruise ships, *i.e.*, those vessels that routinely, as part of their normal operating procedures, carry passengers. While we recognize that some cargo vessels may also, at times, carry passengers, we do not feel it is appropriate to expand this provision to other categories of vessels at this time. We feel that appropriate flexibility is given in the interpretation of ''escort'' to address these situations, while maintaining security. Additionally, facilities are already able to designate certain portions of their facility as ''public access areas,'' therefore we do not feel it necessary to expand the ''passenger access area'' concept to facilities at this time.

Several commenters recommended that the definition of ''passenger access areas'' be clarified in the final rule to state that no person, including employees, workers, and vendors, would need a TWIC to have unescorted access to a passenger access area on a vessel.

We have not amended the language as suggested, but agree with the commenters' concept. The proposed, and now final, definition of ''passenger access area'' states that these areas are not part of the secure area of the vessel. Thus, anyone requiring unescorted access to the passenger access area ONLY does not need to have a TWIC,

as he or she does not need unescorted access to a secure area. This covers passengers, employees, other workers, and vendors.

(d). Monitoring

One commenter felt that the definition of ''monitoring'' as used in current regulations and the TWIC NPRM, was ambiguous, confusing, and should be deleted. We disagree. The NPRM did not propose to change the definition of monitoring, and as such we are not making any changes in the final rule. For an explanation of what was meant by that term, *see* the final rule titled ''Implementation of National Maritime Security Initiatives,'' issued on October 22, 2003 (68 FR 60448).

(e). Breach of Security

One trade association recommended that the definition for ''breach of security'' as used in current regulations and the TWIC NPRM be clarified to allow certain individuals without a TWIC in secure areas, such as escorted persons and foreign seafarers conducting authorized ship's business. The commenter also recommended that the guidance in parts 104 through 106 be amended to clarify this.

Neither the NPRM nor the final rule amend the definition for ''breach of security.'' As stated in the NPRM, ''[c]ircumstances that trigger the reporting requirement[s] in § 101.305 are highly fact-specific and difficult to define comprehensively.'' (71 FR 29417). Generally speaking, finding properly escorted persons within a secure area would not, in and of itself, constitute a breach of security. One situation that would, with certainty, however, is finding someone unescorted within a secure area without a TWIC. This would constitute a breach of security. We will be issuing new guidance for parts 104 through 106, in the form of a NVIC, and will be sure to include provisions on what could constitute breaches of security or suspicious activity in the context of TWIC.

(f). Escorted/Unescorted Access

Several comments requested clarification and additional guidance on the definition of ''escorting.'' Several commenters requested additional clarification about the level of surveillance for personnel without a TWIC, and supported the use of surveillance and monitoring technology instead of physical escorting, or the use of one escort to monitor multiple individuals. The commenters said that constant, one-on-one supervision would be unduly burdensome.

Commenters also stated that the escorting and recordkeeping requirement would be too burdensome in terms of manpower, cost, and recordkeeping. Many of these commenters interpreted the definition to require the physical presence of one escort for each individual without a TWIC at all times while in a restricted area. Some of these commenters provided examples of situations where the requirement would be too burdensome. One port authority stated that it typically has over 100 temporary workers on site that would require escorts. Another commenter was concerned that the rule may prevent shore leave for European Union workers not holding a TWIC, particularly where an escort was unavailable or the regulations were interpreted inconsistently at different ports. One trade association felt that the requirement for escorting would be too burdensome for facilities without the manpower to escort individuals without TWIC, particularly in emergency situations when the workforce has been displaced. One commenter felt that the escort provisions should be unnecessary for foreign maritime facilities complying with the International Ship and Port Facilities Security Code (ISPS Code).

Several commenters were concerned about the need to escort repairmen, maintenance crews, truck drivers, delivery men, crews doing dockside checks of their vessel, musicians, caterers, and other workers, and the need for escorting during weekends and non-business hours when escorts might not be available. One commenter stated that it would have to provide escorts for technical representatives of foreign equipment manufacturers to work on its foreign-built (but U.S.-flagged) vessels. The company also said the rule would be ''problematic'' because it would require a constant escort for foreign owners of U.S.-flagged vessels who visit the vessels. They also stated the rule might disadvantage U.S. ship management companies that operate U.S.-flagged vessels for foreign owners.

As noted above in the section discussing changes to the Coast Guard provisions, we have amended the definition of escorted access to clarify that when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, side-by-side escort. Whether it must be a one-to-one escort, or whether there can be one escort for multiple persons, will depend on the specifics of each vessel and/or facility. We will provide additional guidance on what these specifics might be in a NVIC. Outside of restricted areas, however, such physical escorting is not required, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted. Again, we will provide additional guidance with more specifics in a NVIC.

Additionally, as discussed above, the reporting and recordkeeping requirements proposed in the NPRM have been removed from this final rule. We will take the comments on these requirements into consideration when we begin a new rulemaking on reader requirements.

One commenter felt that the definitions of ''escorting'' and ''unescorted access'' are in conflict, and recommended that the definition of ''unescorted access'' be broadened to include either an escort or monitoring sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.

One commenter felt that the definition of escorting was in conflict with the requirement in § 105.290(d) to provide additional security to monitor holding, waiting, or embarkation areas, because passengers that do not hold TWICs may be in those areas. The commenter expressed concern that this conflict could result in inconsistent requirements, with some government officials requiring each passenger to be accompanied one-on-one by security personnel.

''Escorting'' means ''ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.'' As stated above, we did not intend for the term escorting to always mean a one-to-one side-by-side escort, and we have added to the definition to clarify that outside of restricted areas, monitoring will meet the definition of escorting. We believe that the requirements in § 105.290(d) are sufficient to meet the definition of ''escorting'' when passengers are in holding, waiting, or embarkation areas so long as the monitoring provisions of the facility's approved security plan are in place.

One commenter recommended that the definition be clarified to state that the escort must hold a TWIC. This would prevent two individuals without TWICs from escorting each other.

We have included the requirement that all escorts be TWIC-holders in the actual access control provisions of parts

104, 105, and 106. We have added language to the definition to specifically state that individuals without TWICs may not enter restricted areas without being escorted by an individual who holds a TWIC, with certain exceptions for new hires.

One port authority recommended that the escorts be limited to a subset of TWIC holders, as is done in the aviation sector, and that a limit on the number of individuals a single person can escort be established. We have no limits on who can serve as an escort, other than the requirement that all escorts hold a TWIC. Owners/operators are free to establish more stringent requirements for their escorts if they so desire. As stated above, we will be issuing a NVIC that will provide more detail on how many individuals each escort can accompany at one time.

One commenter requested clarification on who was qualified to be an escort and was concerned that they would need to use an outside security service to serve as escorts. It is not our intention to require outside security services in order for an owner/operator to be able to provide escorts. We will provide more guidance on what is expected of escorts in our NVIC, but generally we expect that any escort be able to respond quickly should any of the individuals that he or she is escorting enter (or attempt to enter) an area they are not authorized to be in or engage in activities other than those for which escorted access was granted.

One commenter felt that the definitions of ''escorting'' and ''unescorted access'' are in conflict, and recommended that the definition of ''Unescorted Access'' be broadened to include either an escort or monitoring sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.

The definition of ''unescorted access'' in the final rule provides flexibility, allowing owners/operators to designate which individuals need unescorted access, which need to be escorted, and which need to be banned from all access based on their individual circumstances. The Federal government will take appropriate action against known or suspected terrorists or illegal aliens, preventing them from gaining even escorted access to secure areas. However those persons who represent ''security threats'' due to past criminal activity may not constitute a risk when escorted.

As we noted above, we did not intend for the term escorting to always mean a one-to-one side-by-side escort. In fact, outside of restricted areas, such side-by-side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be found in an area where he or she has not been authorized to go. As stated above, we will provide additional guidance with more specifics in a NVIC.

(g). Recurring Unescorted Access

Many commenters supported the provision allowing the holder of a TWIC who regularly enters and departs a secure area on a vessel on a continual basis to do so without verifying the TWIC for each such event. The commenters felt that screening employees that access secure areas frequently would be burdensome. One commenter stated that this provision is needed by operations with few employees. Some of these commenters supported expanding this provision to include facilities. One commenter recommended that facilities allow recurring unescorted access without TWIC verification, when the validity of an individual's TWIC has been confirmed within the prior thirty days during Maritime Security (MARSEC) Level 1, but that at MARSEC Level 2 TWIC verification be conducted each time the individual accesses the area.

One commenter recommended the definition be revised to ''* * * authorization to enter a vessel or facility on a continual basis after an initial personal identity and credential verification, as outlined in the vessel or facility security plan.'' The commenter stated that this modification will provide significant relief for facilities during MARSEC Level 1.

We reviewed these comments and recognize that recurring unescorted access might be a valuable and sensible tool for both vessels and facilities. However, because the requirements for readers and owner/operator TWIC verification have been removed from the access control provisions of this final rule, the term is no longer used within the access control provisions of subchapter H. Despite this fact, we have retained the definition, and expect that it will be used in a future rulemaking to impose reader requirements. Any NPRM on that issue will include consideration of expanding the concept to any vessel or facility with a small enough contingent of regular employees that allowing such access would not present a significant security risk.

(h). Secure Area

There were numerous comments on the proposed definition of secure area. One commenter requested clarification on where card readers need to be located for secured and restricted areas. When the NPRM on reader requirements is published, we will include clarification on this subject, where appropriate.

Many commenters felt that the use of the terms ''secure area'' and ''restricted area'' was confusing, and that additional clarification or changes to the definitions or use of these terms be made. Several commenters believed that these terms meant the same thing, and recommended using either ''secure area'' or ''restricted area'', but not both. Several commenters felt that ''secure area'' should not be defined as ''restricted area'' at low consequence facilities. One commenter recommended that any facility be given the flexibility to designate its existing restricted areas as its secure areas in its TWIC Addendum. The commenter recommended that specific provisions in the proposed regulations that could be interpreted as preventing this, such as the requirement that ''appropriate personnel know who is on the facility at all times'' (33 CFR 105.200(b)(18)) and the record keeping requirements (33 CFR 105.225(b)(9)) should be revised to make it clear that they only apply within the secure areas designated in the TWIC Addendum. One commenter recommended that only the term ''secure area'' be used, while other commenters recommended that only the term ''restricted area'' should be used. Many commenters recommended that the definition of ''secure area'' should be aligned with, or made the same as, the existing definition of ''restricted area'' used in existing security plans. The commenters felt that this would be more consistent with existing regulations and security plans and would allow flexibility without reducing security. These commenters argued that having different definitions would result in unnecessarily increasing access restrictions in areas that are restricted to employees only but are not essential for security, such as galleys and storage areas. Some commenters recommended that the final rule include a definition of ''employee only area'' or ''owner-controlled area'' for such areas, and that TWIC not be required for them.

Two commenters recommended that the term ''secure area'' be defined more narrowly than ''restricted area.'' One of these commenters was concerned that defining the terms ''secure area'' and ''restricted area'' to be the same would be costly for facilities and vessels that have designated in their security plan their entire facilities and vessels as a ''restricted area.''

Several commenters recommended that if ''secure area'' and ''restricted area'' are defined as coextensive, facilities should have flexibility in determining which ''secure areas'' require TWIC. Another commenter recommended that if ''secure area'' and ''restricted area'' be defined as coextensive, the agency create a definition for ''security sensitive areas'' requiring TWIC that would be a subset of ''secure areas.'' Multiple commenters requested that if these terms do have different meanings, the final rule should explain the difference, and identify the difference in access restrictions required for them.

One commenter was concerned that the Coast Guard would not accept the ''restricted areas'' established in existing security plans as ''secure areas.'' This commenter felt that vessels and facilities should have the flexibility to define existing areas designated as ''restricted areas'' as ''secure areas'' to avoid expending resources on areas that are not important to security.

Multiple commenters were concerned that the definitions of ''secure area'' or ''restricted area'' would result in inconsistent application by regulators at different facilities. One commenter was concerned that their entire facility has been determined to be a secure area, and thus all of their employees would require a TWIC. Some commenters recommended that small facilities be allowed to define areas as being ''secure areas'' only when a vessel is present.

Several commenters were concerned that the definition of ''secure area'' was too broad, and would require TWIC for any area with any access restriction, such as a fence. Commenters were concerned that this would result in their entire vessel or facility being designated as a ''secure area.'' Many of these commenters felt that they could not meet such a requirement, or that such a requirement would be unnecessary for security. One commenter expressed concern that this might result in numerous Transportation Security Incidents.

One commenter recommended that the first sentence of the proposed rule be rewritten to read, ''Secure area means the area on board a vessel or at a facility or outer continental shelf facility which the owner/operator has designated as requiring a transportation worker identification credential (TWIC) for a person obtaining unescorted access, as defined by a Coast Guard approved security plan.''

Multiple commenters recommended that the final rule clarify that facility owners and operators have broad flexibility in designating ''secure areas,'' and that the Coast Guard readily approve such designations. These commenters felt that this was necessary to minimize the costs and disruptions from the rule.

One commenter recommended that the proposed rule be amended to include a process for limiting the portions of sites to be covered by the rule based on security vulnerability criteria, which would certainly include barge unloading facilities and possibly other areas designated as ''restricted'' in the site's FSP developed under MTSA.

As noted above in the discussion of changes to the Coast Guard provision of this rule, we did not intend for the terms ''secure area'' and ''restricted area'' to be read as meaning the same thing.

As also noted above, we recognize that many facilities may have areas within their access control area that are not related to maritime transportation, such as areas devoted to manufacturing or refining operations. The individuals working in these non-maritime transportation areas may rarely, if ever, have a need to access the maritime transportation portions of the facility. As such, we are giving facility owners or operators the option of amending their FSP to redefine their secure area to include only those portions of their facility that are directly related to maritime transportation or are at risk of being involved in a transportation security incident. Redefining the secure area does not necessarily reduce the original facility footprint covered by the FSP where security measures are already in place. That can only be achieved by a reevaluation of the facility as a whole. Instead, the amendment will only effect where TWIC program requirements will be implemented. Additionally, any secure areas must have an access control perimeter which ensures only authorized individuals with valid TWICs have unescorted access. These amendments must be submitted to the cognizant COTP by July 25, 2007.

One commenter expressed a desire for Coast Guard to support allowing a facility owner/operator to modify their FSPs by maintaining a significant level of security for the entire facility, while enhancing security for narrower area of the site. This commenter proposed the following language for the final rule preamble: ''Facility owner/operators are encouraged to review, and revise as necessary, their Facility Security Plans to apply TWIC requirements to those portions of the site that (i) trigger MTSA regulation, (ii) can be reasonably separated through access controls from other parts of the facility; and (iii) require a higher degree of security protection. Coast Guard will review and approve these changes to the FSP so long as the facility demonstrates that (i) it can maintain existing security at the balance of the facility, and (ii) restricted access controls (including TWIC access controls) have been provided for the area that will have heightened security.''

We agree with the substance of this comment. While the exact recommended verbiage has not been incorporated into the final rule, we believe the intent and proposed flexibility has. Facility owners and operators will continue to be responsible for drafting and submitting their unique security plans for Coast Guard approval. As noted above, greater flexibility has been afforded to facility plan submitters, allowing them to redefine their secure area to include only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident.

We realize that there may be some owners and operators of vessels that would like the same option. However, vessels present a unique security threat over facilities in that they may not only be targets in and of themselves, but may also be used as a weapon. Due to this fact, we will continue to define the entire vessel as a ''secure area,'' making exception only for those special passenger and employee access areas which are discussed below. Vessel owners/operators need not submit an amendment to the VSP in order to implement these special areas, however they may do so, following the procedures described in part 104.

Commenters also requested clarification on whether the term ''secure area'' is intended to include passenger access areas as defined under 33 CFR 105.106. These commenters recommended that the passenger access areas not be defined as ''secure areas.''

''Passenger access areas'' are, by their definition, not secure areas. They will, however, exist solely within the secure area of the vessels on which they are implemented. As such, they will operate as ''pockets'' within the secure area.

One commenter stated that small passenger vessels and facilities where they moor would be at a small risk of a terrorist attack. The commenter recommended that the final rule state that such vessels and facilities do not have any ''secure areas.''

We do not agree with this comment. During the MTSA rulemaking process, the Coast Guard evaluated all vessels and facilities to determine which of those are at a high enough risk of a

Transportation Security Incident (TSI) to warrant imposing the security plan requirement. Small passenger vessels and the facilities that they use were determined to pose a high enough risk to warrant imposition of the security plan requirement. We do not believe that circumstances have changed to warrant a change to those requirements. We have, however, provided some relief to small passenger vessels in this rulemaking by allowing them to carve out passenger and employee access areas (explained elsewhere in this final rule), which will help minimize the ''secure area'' on board.

One commenter was concerned that since secure areas are defined in the owner or operator's threat assessment (which is approved by the Coast Guard, but is not publicly available), a business operating at the port, vessel, or facility for the first time would not know what areas are designated as ''secure'' and whether they need a maritime TWIC.

The threat assessment approved by the Coast Guard addressed restricted areas, not secure areas. We have defined secure areas as the access control areas of vessels and facilities, which should provide enough guidance to new businesses, as the area over which a vessel or facility exerts access control should be readily visible to anyone approaching that vessel or facility for access.

One commenter also requested clarification on whether ''secure areas'' corresponds to existing security classification existing under the ISPS Code.

The comment is unclear. The ISPS Code uses the term restricted area, and as discussed above, we do not intend for the secure area to mean the same thing as restricted area. In that regard, this final rule does not correspond with the ISPS Code. However, we note that the definition we have provided will not interfere with a vessel or facility meeting the requirements of the ISPS Code.

One commenter noted that safety issues surrounding needed access to ''secure areas'' in an emergency are not addressed. Another commenter stated that access to secure areas cannot be restricted in an emergency. We recognize this issue and have added a paragraph to § 101.514 that clarifies emergency personnel need not have TWICs to obtain unescorted access to secure areas during emergencies.

Two commenters recommended that the term ''secure area'' be revised to read ''Secure area is used as defined in 33 CFR 101.''

We disagree. The definitions found in 33 CFR part 101 apply to all of subchapter H, therefore it is not necessary to constantly refer back to part 101 when, in parts 103 through 106, we use a term defined in part 101.

2. General Comments on Applicability

Many commenters had questions and/or concerns for TSA and Coast Guard related to the applicability of the proposed rule. One asked what the TWIC requirements would be for a CDC facility that is in a separate location on port property, since it is not a secure maritime facility and thus does not fall under the security regulations of 33 CFR part 105.

Another commenter posed several questions for TSA and Coast Guard: Will the unlicensed crew members on small passenger vessels certificated for less than 150 passengers under ''Subchapter K'' need to hold a TWIC? Will unlicensed crew members on passenger vessels carrying more than 12 passengers, including at least one passenger-for-hire, on an international voyage, which can include large charter yachts of up to 500 Gross Register Tonnage (GRT), be required to carry a TWIC? Will deckhands on barges subject to ''Subchapters D or O'' be required to obtain a TWIC? Will deckhands on towing vessels greater than 26 feet in length be required to obtain a TWIC?

One commenter noted that every terminal under MTSA is unique, which is why they are required to have FSPs and suggested that 33 CFR part 105 be used as a baseline and to allow terminals to write their specific plans to ensure security and ease of commerce thus allowing the terminal operators to determine if individuals without the TWIC may have unescorted access to the terminal. One commenter shared their experience implementing legislation similar to the TWIC via Florida Statute 311.12. The commenter suggested adding a grandfather component to the proposed rule to allow current personnel working in the maritime industry certain considerations. The commenter went on to note that if they had not implemented a grandfather component to Florida Statute 311.12, the smooth operation of commerce would have come to a halt.

Many commenters, including individuals, marine services companies, barge lines, cruise lines, towing companies, and marine maintenance companies, argued that they already had adequate security plans, restrictions, testing procedures, personnel procedures, and other safeguards in place, some of which were approved by the Coast Guard. One local government commenter said that TSA should exempt any facility from the TWIC requirements that had a FSP already in place. Another commenter noted that in the absence of security incidents at any scrap yards relating to maritime transportation and small port facilities that receive bulk aggregate materials, the FSP should be sufficient for addressing risks at such facilities.

MTSA was clear and unambiguous, leaving little if any room for agency interpretation. Essentially, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA regulated facilities or vessels. In addition, the statute was very clear that all credentialed Merchant Mariners will be issued a biometric identification card, which will be the TWIC. Where needed and allowable under the statute, certain arrangements or exemptions were proposed and modified as the result of the public comments to identify special cases where individuals without a TWIC or who are unable to obtain a TWIC can continue to work aboard MTSA regulated facilities or vessels, subject to additional security provisions.

As a result of the public comments and concern regarding the potential negative impact on industry resulting from the requirements to implement a TWIC system, greater flexibility has been afforded to facility owners/operators by allowing them the option, in revised § 105.115, to redefine their ''secure area'' as only that portion of their access control area that is directly related to maritime transportation. Other definitions, such as ''passenger access area'' and ''employee access area,'' will also provide greater flexibility in assisting regulated entities with enhancing security while meeting the new regulations. Additionally, provisions have been included, as discussed more specifically below, to allow limited access to new hires under specific conditions, and to persons who have reported their TWIC as lost, damaged or stolen and are awaiting replacement cards.

One commenter recommended utility fuel-handling facilities be the only facilities subject to the TWIC program. The commenter also recommended that the TWIC be required for such facilities only when the facility is being used for off-loading.

As stated earlier, the MTSA of 2002 clearly and unambiguously ruled out blanket waivers for specific industry segments or specific job descriptions. With very limited exceptions, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA regulated facilities or vessels.

(a). Applicability—Requests for Exemptions

Numerous commenters requested exemptions from the TWIC requirements for the following industries, vessels, and facilities:

- U.S.-flagged passenger vessels;
- U.S.-flagged mobile offshore drilling units (MODUs) and offshore supply vessels (OSVs) operating outside the geographic boundaries of U.S. jurisdiction, employing non-citizen workers;
- Other U.S. flagged vessels employing non-citizen crewmembers under the provisions of 46 U.S.C. 8103(b)(3) or (e);
- Inland tugboat, towboat, and barge industry;
- Small and/or isolated low consequence ports, facilities, or vessels;
- Facilities with security requirements that are equivalent or more stringent than the TWIC (*e.g.*, shipyards that currently meet existing DOD credentialing and security plan requirements);
- Facilities and vessels participating in aggregate stockpile and loadout activities;
- Tall ships operating under the U.S. flag and educational sailing programs for school children;
- Bunkering and gas support facilities; and
- U.S. vessels undergoing repairs at a foreign port or facility.

The commenters presented various arguments to support their requests for exemption. Some commenters noted that exemption criteria should be added to the proposed rule indicating that vessels and facilities that were deemed low risk during a risk assessment should not fall under the TWIC requirement, because TWIC places an unwarranted burden on these vessels and facilities with little added security benefit. For example, one commenter requested that oil and gas support facilities and bunkering facilities be exempted from the TWIC requirements. Another commenter asked for an exemption since their activities and their location are low risk, predominately carrying bulk and break bulk products within the Great Lakes.

Similarly, other commenters argued that small vessels (*e.g.*, inland towing vessels, small passenger vessels) or small ports should be exempt from the TWIC requirements because the workers know each other and unknown visitors are infrequent. These commenters argued that the intent of the TWIC system, to identify those people who pose a threat, would not be served by installing card readers on small vessels or in small ports. They stated that identifying someone who does not belong is not difficult on these small vessels and in these small ports, and can be accomplished visually. They claimed that the proposed rule would only add cost to these industries with little to no benefit to maritime security. For example, many commenters noted that the crews on inland towing vessels are predominantly U.S. nationals who already comply with the security regulations in 33 CFR parts 104 and 105, so requiring TWICs for this industry would be costly and would result in few improvements in maritime security. In addition, several commenters from the small passenger vessel industry requested that subchapter K and T vessels operating in restricted waters and routes be exempt from the proposed rule.

More specifically, some commenters noted that vessels under a specific tonnage should be exempt from the TWIC requirements. One commenter asked that vessels of less than 500 regulatory tons GRT and 6,000 International Tonnage Convention (ITC) tons be exempt from the requirements. Another commenter asked that vessels less than 100 gross tons with undocumented workers be exempt from the proposed rule.

Many commenters argued that U.S.-flagged MODUs and offshore supply vessels (OSVs) operating outside the geographic boundaries of U.S. jurisdiction, employing non-citizen workers should not be required to obtain a TWIC. One commenter argued that in some countries the law requires these vessels operating on the continental shelf to hire local crewmembers, so requiring escorts for all of these crewmembers would place a large burden on these vessels and cause them to be unable to work overseas. In addition, the commenters argued that there is little threat posed by these vessels that are located thousands of miles from the U.S. coast. More than one commenter stated that the ISPS Code and its implementing regulations in SOLAS recognize the need for MODUs and OSVs to employ non-U.S. citizens in their crew and apply shelf-State standards instead of flag-state standards. The TWIC program should recognize the need for these vessels to employ non-U.S. citizens as well.

One commenter stated that it is their understanding that foreign-flagged MODUs (OCS facilities) that are on location on the OCS would be excluded from the requirements, since foreign vessels with valid ISPS Code certificates are in compliance with 33 CFR part 104 (except 104.240, 104.255, 104.292, and 104.295) and all foreign vessels are exempt from TWIC requirements under 33 CFR 104.105(d). The commenter asked for confirmation that this understanding of the proposed rule is correct. In addition, they requested confirmation that a MODU that is not regulated under part 104, and therefore not required to implement TWIC provisions, but is working next to or over an OCS facility that is regulated by part 106, and therefore is required to implement TWIC provisions, would be exempt from the TWIC requirements.

In addition to requests for exemptions for industries, vessels, and facilities, many commenters requested exemptions for the following types of workers:

- Employees who work at small ports, facilities, or vessels;
- Merchant seamen who are U.S. citizens and hold current U.S. Coast Guard licenses, Merchant Mariner Documents (MMD), certificates of registry, and STCW documents;
- Employees on vessels under 100 gross tons;
- Contract security guards who have already undergone a DOJ background investigation;
- Crewmembers, service technicians, or repair persons performing vessel maintenance and repairs;
- Hotel staff and passenger vessel staff;
- Seasonal or short term workers which access needs of less than 90 days;
- Cadets from U.S. maritime academies;
- Emergency response personnel;
- 15.702(b) crew and other authorized foreign nationals boarding U.S. vessels overseas;
- Employees who must continuously enter and exit secure areas (*e.g.*, baggage handlers at a cruise ship terminal);
- Port chaplains or other religious personnel;
- Workers who are not involved in the transportation industry; and
- Vessel agents.

The reasons presented by the commenters for granting the workers' an exemption were varied. Some commenters argued that passenger vessel staff who work within the same areas as the passengers who are not subject to the requirement should not be required to obtain a TWIC.

Commenters argued that crewmembers, service technicians, or repair persons performing vessel maintenance and repairs should not be required to obtain a TWIC because they do not present a security risk and additionally because there are not enough vessel and facility staff to escort these workers.

One commenter asked that the proposed provision exempting foreign vessels be expanded to also exempt ''foreign nationals employed on U.S. vessels under the provisions of 46 CFR 15.720(b) or who are authorized visitors aboard a U.S.-flagged vessel operating from or in foreign ports.''

Many commenters requested exemptions for emergency response personnel and law enforcement officers.

More generally, commenters suggested that workers should be exempt from the TWIC requirements until they go to work for a company that needs to conduct business in a secure area. In addition, commenters requested that workers without access to restricted areas of vessels or terminals not be required to obtain a TWIC.

MTSA was clear and unambiguous and ruled out blanket waivers for the requested industry segments or specific job descriptions. Essentially, all individuals must hold a TWIC in order to be eligible for unescorted access to secure areas of MTSA-regulated facilities or vessels. Where needed and allowed by statute, certain arrangements or exemptions were proposed and modified as the result of the public comments to identify special cases where individuals without a TWIC or who are unable to obtain a TWIC can continue to work aboard MTSA-regulated facilities or vessels subject to additional security provisions.

These special cases include the foreign vessel exemption, a new provision within the definition of secure area stating that in certain circumstances, U.S. vessels operating in foreign waters do not have secure areas, the passenger and employee access areas, and the provision allowing part 105 facilities to amend their security plans to limit their secure area to only those portions of their facility that are related to maritime transportation.

When issuing the regulations found in 33 CFR chapter I, subchapter H (known as the Coast Guard MTSA regulations), which establish who must submit a security plan, the Coast Guard utilized a risk based approach to identify and separate those particular facilities and vessels which pose a higher risk from those which pose a lower risk. While we agree with the argument that one MTSA-regulated facility or vessel can pose a lower risk than another MTSA regulated facility or vessel, the fact remains that all have already been determined to present a high enough risk of a TSI to warrant their inclusion in the MTSA regulations. The statute requires all MTSA regulated vessels and facilities to comply with the access control requirements by requiring TWICs for unescorted access to secure areas.

As a result of numerous comments and concerns regarding reader usage and installation aboard facilities and vessels in addition to emerging technology, this final rule addresses use of the TWIC as a visual identity badge and does not require use of readers. We will consider those comments requesting that the risk among all MTSA regulated vessels and facilities be reevaluated when we propose reader standards in a subsequent rulemaking.

Understanding the unique situations where successful commerce and support of the maritime industry is dependent upon legal employment or boarding of foreign mariners or crew while operating outside of U.S. waters, we determined that we must change some language from the proposed rule. As such, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provisions found in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

Additionally, facility owners/operators can affect the population of those who will need to obtain a TWIC by taking advantage of the option given to them in revised § 105.115 and redefining their ''secure area'' as only that portion of their access control area that is directly related to maritime transportation. The Coast Guard must approve such modifications.

(b). Applicability—Foreign Vessels

One commenter supported the proposed exemption for foreign flag vessels calling on U.S. ports. The commenter stated that this would include not requiring a valid TWIC to access vessel-designated restricted areas and the need for TWIC readers aboard foreign flag vessels. However, many commenters disagreed with this provision for various reasons. Some commenters stated that there is a need for application of international standards to all ships, U.S. and foreign, to maintain a level playing field and prevent economic discrimination against U.S. ships. For example, one commenter stated that security within the Gulf of Mexico will not be ensured until the foreign vessels that routinely operate in support of the offshore oil and gas industry, and call on Gulf ports such as Fourchon, Galveston, Mobile, etc., are held to and comply with equivalent standards.

Another commenter urged that an accurate cost-benefit analysis must factor in the cost of vessel operating companies that are forced out of business because they cannot compete with foreign competitors in the Gulf of Mexico who have been exempted from these requirements.

Other commenters argued that the proposed regulations overlook the area of greatest interest to national security, namely the traffic of foreign vessels and foreign seafarers at U.S. ports and maritime facilities, while imposing additional regulation on American mariners who already undergo thorough vetting, and U.S. vessels that already operate under a vessel security plan compliant with the MTSA. One commenter claimed that a security threat posed by individuals on a foreign-flagged vessel moored at a U.S. port is no less of a security threat than persons aboard a U.S. vessel, and objected that TSA has decided to forgo security requirements for foreign-flagged vessels. One commenter expressed that DHS has not conducted any analysis as to whether foreign mariners who do not participate in SOLAS or ISPS pose homeland security threats. One commenter stated that the Coast Guard has not fully considered the impact of its requirement to grant access to foreign nationals who have not been vetted by TSA.

One comment stated that because foreign mariners are not required to hold a TWIC under the proposed rule, if the entire terminal is classified as a ''secure area,'' crewmen that have docked at berth and have been cleared by CBP must be escorted every time they leave the ''restricted area'' of the pier. The commenter notes that if they are already in the restricted area they do not have to be escorted, but if they enter that part of the secure area that is not restricted, they must have an escort. The commenter asked that, since CBP has already made a determination whether these mariners pose a risk to our country, why then does a low consequence terminal have to make sure they are escorted if they pose no risk?

One comment said the proposed rule does not clearly indicate whether a foreign vessel must obtain, deploy, and operate TWIC readers at its access points on the vessel. However, the commenter said that the proposed rule appears to exempt foreign vessels from using TWIC readers.

Foreign vessels carrying valid ISPS Certificates do not fall within the TWIC applicability of the MTSA, as they are not carrying security plans approved by

the Secretary under 33 U.S.C. 70103. MTSA requires compliance with TWIC requirements for vessels or facilities whose plans include an area designated as a secure area by the Secretary for purposes of a security plan approved under sec. 70103. The vast majority of foreign vessels do not submit their plans to the Secretary, and therefore are not ''secure areas'' even when the foreign vessel is docked at a U.S. port. However, when docked at a U.S. port, individuals on the foreign vessels are subject to the facility's security plan—including TWIC and escorted access requirements—if they wish to leave the foreign vessel.

We do not agree that sec. 102 of the MTSA applies to foreign seafarers arriving on foreign vessels. The TWIC process cannot practically or meaningfully be applied to foreign mariners, who would not likely have the means to get to enrollment centers or to return to claim and activate their credentials, nor would any be able to present the appropriate identity documents, or meet the requirement for lawful presence. Requiring foreign seafarers to present a TWIC would mean that before being allowed off of a foreign vessel, each foreign seafarer would need to come to the United States to enroll in the TWIC program, and then again to pick up their TWIC. It is also not clear that such a provision would provide any security benefit, as the criminal background checks that are done as part of the TWIC security threat assessment would have very little meaning, since it is unlikely that a foreign seafarer will have a criminal record in the United States, and the additional background checks are done during the visa application and CBP screening processes (see below). Finally, placing such requirements on foreign seafarers would certainly affect the treatment U.S. mariners receive in other countries.

We also disagree that the TWIC subjects U.S. maritime workers and mariners to stricter processes than foreign seafarers. Currently, foreign seafarers arriving on foreign vessels are required to have a U.S. visa, issued by the Department of State subsequent to at least one face-to-face interview and a vetting process that is similar to TWIC vetting. Upon arrival in the U.S., foreign mariners are not allowed to leave the vessel until and unless they are allowed entry after inspection by a CBP Officer. Those seafarers that arrive without a visa or a CBP issued waiver are restricted to the vessel. Seafarers that are allowed to leave the vessel are subject to the security provisions of the facilities where their vessel is moored, including the conditions by which they are allowed to traverse the facility, and will be required to have escorted access through secure areas of the facility.

One commenter urged that a further provision be added at new § 104.105(e) to read as follows: ''(e) Foreign nationals employed on U.S. vessels in accordance with the provisions of 46 CFR 15.720 or who are authorized visitors aboard U.S. flag vessels operating from or in foreign ports are not subject to the TWIC requirements found in this part.''

As noted above, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provisions found in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas. These waiver provisions allow U.S. vessels to employ foreigners as crew in certain circumstances. The effect of this change is to exempt these vessels from the TWIC requirement while they are operating under the referenced waivers. As soon as the vessel ceases operating under these waiver provisions, it will be deemed to have secure areas as otherwise defined, and TWIC provisions will apply.

Many commenters stated that not requiring foreign vessels and foreign crews to obtain a TWIC would be detrimental to U.S. maritime security. One commenter noted that this policy would put U.S. offshore oil and gas supplies at risk. One commenter pointed out that currently a large portion of the ships transporting oil and hazardous materials are foreign vessels with foreign crews.

Another commenter noted that 95 percent of the vessels sailing from international waters into U.S. ports are crewed by foreign mariners, so although vetting these foreign mariners would be very difficult it is necessary to enhance U.S. port security. The commenter pointed out that U.S. mariners are already subject to background checks during the licensing procedure, so including U.S. mariners, while exempting foreign mariners from the TWIC program will not enhance U.S. port security.

Numerous commenters expressed concern about uncredentialed foreign mariners. One argued that if licensed and documented American mariners must hold a TWIC, foreign workers on American flag vessels should also be required to hold proper security credentials. Many commenters argued the necessity of covering foreign nationals working as drivers in domestic facilities such as ports and foreign crewmen on foreign vessels, such as Liquified Natural Gas (LNG) tankers. Comments came from a wide variety of maritime and trucking industry associations, and individuals.

Some commenters also stated that ensuring the security of freight moving in from foreign ports was a more important issue than TWIC.

One commenter noted that under the proposed rule many commercial fishing vessels will not be required to obtain a TWIC. The commenter argued that the TWIC program should include all commercial vessels, since commercial fishing vessels could easily be used as a terrorist target.

We do not agree with these comments. As discussed above, the vast majority of foreign vessels are not required to have a security plan under MTSA and thus do not constitute secure areas for purpose of the TWIC program. In regard to the security concerns cited by the commenters, however, individuals from foreign vessels who wish to leave the vessel while docked at a U.S. port are required to be escorted through secure areas on MTSA-regulated facilities. Further, each and every foreign mariner wishing to step off of a vessel onto U.S. soil must be issued a visa from the Department of State, and be admitted by CBP into the United States.

In addition, the Federal government has a variety of programs in place to identify potential security risks from foreign vessels and crew members entering U.S. ports. For example, the Coast Guard's Notice of Arrival requirements (33 CFR part 160, subpart C), U.S. Coast Guard Port State Control Examinations, vessel escorts, and crew list, cargo and last port of call screening, foreign port inspections and similar programs have been in place for several years to reduce the risk posed by certain foreign-flagged vessels transiting or calling U.S. ports.

Additionally, under CBP's Advance Passenger Information System (APIS) (19 CFR 4.7), vessels (both foreign and U.S.-flagged), must provide manifest information on all passengers and crew no later than 24 hours and up to 96 hours prior to the vessel's entry at a U.S. port. The data that must be provided by the vessel to CBP includes: the country that issued the passport or alien registration number; the passenger's or crew member's full name, date of birth, passport or alien registration number, country of residence, visa number, originating foreign port and final port of destination. *Id.* The manifest information is compared against terrorist watchlist information by CBP.

Commercial fishing vessels are not subject to 33 CFR subchapter H and therefore are not included in the congressional mandate for TWIC. As noted in the interim final rule published on July 1, 2003, titled ''Implementation

of National Maritime Security Initiatives,'' commercial fishing vessels were determined to be at a low risk of a TSI during the initial risk assessment and therefore were not included in the applicability for 33 CFR subchapter H (*see* 68 FR 39246–7).

One commenter stated that there are many reasons for foreign seafarers to be allowed to traverse the facility (*i.e.*, reading draft marks, completing a Declaration of Security (DoS), required training, making phone calls, medical and humanitarian needs). The commenter argued that to only mention crew changes and shore leave does not advise facility operators and Federal officials that there are other legitimate reasons for seafarers to be granted access to portions of a facility.

We agree that there are legitimate reasons for foreign seafarers to require limited access to facilities. Recognizing, in particular, that seafarers, whether foreign or U.S., will require access to facility areas to conduct vessel operations, such as reading drafts, adjusting mooring lines, securing shore ties, completing a declaration of security (DoS), and loading stores, we have included a provision to allow mariners limited access immediately adjacent to their vessels to conduct these operations. Limiting the access in this manner takes operational realities into account without adversely impacting security. Also recognizing this need applies to U.S. vessels not covered by 33 CFR part 104 when moored at a part 105-regulated facility, this provision is also granted to U.S. mariners on vessels not covered by part 104 who would not otherwise be required to possess a TWIC.

(c). Applicability—Mariners

One commenter requested clarification about whether every uncredentialed mariner (*e.g.*, crewmember) requiring unescorted access to secure areas of vessels and facilities will require a TWIC. Many crewmembers who have unescorted access to secure areas of vessels and facilities are not required to have credentials (*e.g.*, up to 17,000 crewmembers on inland and river towing vessels up to 1,600 GRT; crewmembers on small passenger vessels up to 100 GRT; and offshore towing vessels up to 100 GRT), noted one commenter. Therefore, the commenter argued that the proposed rule needs to make it clear that every uncredentialed mariner requiring unescorted access to secure areas of the vessels (especially small passenger vessels, offshore supply vessels or facilities) will need a TWIC.

Under this rule, every mariner, whether holding a credential from the Coast Guard or not, who requires unescorted access to a secure area of a MTSA-regulated vessel or facility will need to have a TWIC.

Another commenter, an owner of vessels and facilities, noted that they currently are not required to have VSPs or FSPs, however, the proposed rule indicates that their licensed employees will now need to obtain a TWIC. The commenter stated that making a licensed employee obtain a TWIC when the workplace is non-secure does not make sense. In addition, the commenter noted that only requiring licensed crewmembers to obtain a TWIC, but exempting unlicensed crewmembers, does not make sense. One commenter suggested that this could become very burdensome for the vessels and facilities, since individuals may choose not to obtain a TWIC and thus will have to be escorted while in secure areas. The commenter recommended that TSA and Coast Guard make the TWIC mandatory.

Many individual commenters and commenters from mariners' associations argued that domestic merchant seamen are already required to obtain documentation, and that an additional burden should not be placed on them. Several said that domestic professional mariners should be considered partners in security, because they have a vested interest in a secure workplace. Commenters stressed that the rule should recognize the difference between ''bluewater'' international operations and ''brownwater'' domestic operations on inland waterways, because the latter do not pose the same threat to national security. Several commenters also argued that the economic effect of the proposed rule would be to place domestic maritime workers, such as those in the offshore oil and gas industry, at a disadvantage vis-à-vis foreign competitors.

The final rule applies to all licensed mariners, regardless of where they work, and workers needing unescorted access to secure areas of vessels, facilities, and OCS facilities currently regulated by parts 104, 105, and 106. Licensed mariners, regardless of their employer or working location, must obtain TWICs due to sec. 102 of MTSA (46 U.S.C. 70105(b)(2)(B)), which states that the TWIC requirement applies to ''an individual issued a license, certificate of registry, or merchant mariners document under part E of subtitle II of this title.'' Additionally, the statute requires that any individual requiring unescorted access to secure areas of a vessel or facility regulated by 33 CFR part 104, 105, or 106 obtain a TWIC, regardless of whether they are licensed or unlicensed. (*See* 46 U.S.C. 70105(b)(2)(A)). We disagree with the commenters who felt that the TWIC requirement was ''not mandatory.'' Mariners will not be able to renew their credentials without a TWIC, and vessel and facility owners/operators have an enforceable responsibility to ensure that only persons holding TWICs be granted unescorted access to secure areas. If an individual shows up for work without a TWIC, and his or her employment would call for unescorted access within a secure area, it is the duty of the owner/operator to either turn that individual away or provide an escort, but there is nothing stating that the owner/operator must allow the individual access of any kind. We have provided for limited exceptions to this, to cover newly-hired individuals who have applied for their TWIC but have not yet received it, and to cover those individuals who have reported their card as lost, damaged, or stolen. These provisions can be found in the access control sections of parts 104, 105, and 106.

(d). TWIC Eligibility—Foreign Workers

Many commenters argued that foreign workers who have already obtained work visas and have been cleared by CBP should be allowed to obtain a TWIC, even though they are not resident aliens. For example, some commenters pointed out that trained foreign experts with work visas are often used on U.S.-flagged industrial vessels to assist with specialized work. The commenters argued that requiring an escort for these workers who have already been cleared by the CBP and obtained the appropriate work visas, would be burdensome and unnecessary. These commenters pointed out that just as the NPRM states that Mexican and Canadian truckers need to have access to facilities, offshore vessels need to allow specialized foreign workers on their vessels. Other commenters stated that the proposed rule is more stringent than what is required by law.

Several commenters noted that as a multinational corporation they have foreign employees and foreign business partners at their U.S. facilities, so if these employees and business partners cannot obtain a TWIC it will create a large burden for their corporations. The multinational corporations will face a burden not only from having to provide escorts for their foreign employees and foreign business partners, but also from lost business due to foreign business partners choosing not to work with U.S. multinational corporations due to the extra hassles.

We recognize that this population of workers is essential to the maritime transportation industry and that there would be significant impacts to facilities if they were not able to obtain unescorted access to carry out their work. As a result, we have amended the final rule to allow additional foreigners, holding certain work visas, to apply for a TWIC. These provisions are discussed in more detail in the TSA section below.

We do not believe, however, that TWICs should be issued to anyone who has been granted a work visa and cleared by CBP. While foreign workers—either immigrant or nonimmigrant—may be subject to certain screening to obtain a visa or to enter the country. However, these individuals do not undergo the comprehensive security threat assessment necessary to allow a person unescorted access to a secure facility.

(e). Applicability—Area Maritime Security (AMS) Committee Members

The NPRM proposed requiring that all AMS Committee members obtain a TWIC. Several commenters stated that they agreed with this provision of the proposed rule. For example, one commenter noted that if the rule is not applied equally to all parties it will have little value. Other commenters stated that they did not agree with this provision and felt that AMS Committee members should not have to obtain a TWIC. Some of these commenters argued that the TWIC is not a tool to clear individuals for access to SSI[21], but is a tool to assist facility and vessel owners in implementing access control. The commenters argued that since some of the AMS Committee members do not need access to secure maritime areas and all of the AMS Committee members have already undergone the screening for access to SSI, the AMS Committee members should not have to obtain a TWIC. In addition, commenters noted that requiring the AMS Committee members to obtain a TWIC would increase the costs associated with membership and thus discourage membership.

After reviewing these comments, we have decided to refine the TWIC requirement in regard to AMS Committee members, as explained above in the discussion of changes to the Coast Guard provisions of the final rule. The final rule allows individuals to serve on an AMS Committee after the completion of a name-based terrorist check from TSA. FMSCs (*i.e.* COTPs) will forward the names of these individuals to TSA or Coast Guard Headquarters for clearance prior to sharing SSI with these members.

(f). Applicability—Owners/Operators

The proposed rule requested comment on whether owners/operators of vessels, facilities, and OCS facilities should be required to obtain a TWIC, based on their access to SSI. Some commenters argued that requiring those who have already been screened for their access to SSI to obtain a TWIC based solely on their access to SSI would be an unnecessary waste of money and resources. These commenters noted that not all SSI is sensitive enough to require the kind of background check that will be a part of TWIC. A few commenters noted that the owner/operator should determine who in their corporation needs to obtain a TWIC and who needs access to SSI. One commenter noted that this question pertains to 49 CFR part 1520, which was not defined as being within the scope of this rulemaking, although it defines SSI and provides standards for access to and control of SSI. Therefore, although 46 U.S.C. 70105(b)(2)(E) permits the Secretary to determine that individuals with access to SSI must have a TWIC, this issue should be the subject of a separate rulemaking addressing the provisions of 49 CFR part 1520. One commenter argued that owners and operators should be subject to the TWIC requirements, since they have access to SSI. Another commenter argued that owners and operators should be required to obtain a TWIC. They argued that owners' and operators' open access to secure areas and SSI by virtue of their position, warrants their need for the TWIC. This commenter went on to argue that not requiring owners and operators to obtain the TWIC would amount to rank discrimination. They sited the Dubai Ports World controversy as further evidence of the need for owners/operators to obtain a TWIC.

The final rule does not include a requirement that all owners/operators obtain a TWIC. We reviewed all of the comments received and agree with the idea that an owner/operator, due to access to SSI access and ability to control the company, should probably go through a background check. However, our difficulty comes in determining who exactly the owner/operator to be checked is. For small or closely-held companies, this is an easy answer, and we expect that in the majority of these cases, the owner/operator will get a TWIC due to his/her need to have unescorted access to the vessel or facility. However, larger, multi-national, publicly traded companies pose a much bigger problem. It would be impractical for TSA to run background checks and issue TWICs to anyone holding stock in a company that may own a facility or vessel regulated under MTSA. Additionally, these companies may be structured in such a manner that a bank or several large holding companies are actually the owners, but they have little to no input on the day to day operations at the facility or vessel. We reiterate, however, that any individual, including owners and operators, who wishes to have unescorted access to secure areas must have a TWIC.

As such, we have not included the TWIC requirement for owners/operators in this rule. We will, however, continue to examine the issue, and may propose adding this requirement in the future.

(g). Applicability—Federal/State/Local Officials

The proposed rule states that Federal officials are not required to obtain a TWIC, but must have an HSPD–12 compliant identification. Several commenters agreed with this provision because to obtain the HSPD–12 compliant identification cards, the applicant is subject to the same or more rigorous level of threat assessment that will be required for the TWIC (*e.g.*, background investigations, fingerprints). Other commenters noted technological issues that will need to be resolved if Federal officials are allowed to use HSPD–12 compliant credentials in place of the TWIC. Several commenters emphasized that it is necessary for the TWIC equipment to be able to read the HSPD–12 compliant credentials or validate the cards' continued validity. Another commenter requested that § 101.514(b) be clarified, so it is clear that Federal officials are still subject to the facility's access control requirements and presenting their credentials does not grant them unescorted access to the facility. In addition, several commenters noted that the proposed rule must include a requirement that Federal officials obtain an HSPD–12 compliant ID on the same schedule as the merchant mariners will be required to obtain TWICs and MMCs.

The final rule will require Federal, State and local officials, in the course of their official duties, to present their current agency credentials for visual inspection to gain unescorted access to secure areas. We recognize the

[21] "SSI" is unclassified information that is subject to disclosure limitations under statute and TSA regulations. *See* 49 U.S.C. 114(s); 49 CFR part 1520. Under 49 U.S.C. 114(s), the Assistant Secretary of TSA may designate categories of information as SSI if release of the information would be detrimental to the security of transportation. SSI may only be disclosed to persons with a need to know, such as those required to carry out regulatory security duties.

technological difficulties presently facing the evolution of the biometric readers. However, in the future, we anticipate a separate rulemaking to require an HSPD–12 compliant credential to be read by a biometric reader for gaining unescorted access. We must stress that Federal, State and local officials will only use their authority to gain unescorted access in the course of their official duties. Such officials must abide by a facility's or vessel's access control requirements unless extenuating circumstances require otherwise.

Under the proposed rule, compliance would be voluntary for State and local officials because the majority of these individuals undergo a security threat assessment prior to beginning their job. However, several commenters argued that this could be detrimental to maritime security and is problematic for several reasons. First, not all State and local officials undergo a security threat assessment. Second, it would be hard for crew members to determine if the State or local official's credential meets TWIC standards. Third, under this provision State and local officials would not be subject to the background check every five years like other holders of the TWIC. Another commenter noted that there have been instances in the past where local and State agencies have conducted their background checks independently of their employee application process. In addition, another commenter noted that the threat of terrorists posing as armed local or State enforcement officers is great, so there needs to be a more thorough evaluation of these individuals' identity then just showing their ID. Several commenters noted that those with the main responsibility for port security (*e.g.*, port authority police who fall under the State and local system) should be required to get a TWIC, rather than make it optional. One commenter specified that all armed law enforcement officials should be required to obtain a TWIC.

One commenter noted that under § 101.514(c) State and local law enforcement officials would not have to possess a TWIC to gain unescorted access to secure areas. At the same time, § 105.210 would require facility personnel responsible for security duties to maintain a valid TWIC. The commenter said that some ports have a police force comprised of certified police officers who are required to obtain the exact training as State and local law enforcement personnel. The commenter recommended that either § 101.514(c) or § 105.210 be rewritten to recognize these port police and remove the requirement for them to obtain a TWIC.

Federal agencies are already required to implement HSPD–12, therefore there is no need for either the Coast Guard or TSA to do more than require that those credentials be used. We believe State and local agencies may issue similar cards as the Federal government completes implementing HSPD–12. Therefore, we are not requiring State and local officials to obtain TWICs at this time. We may revisit this decision in the future. While all State and local officials may not be required to undergo a security threat assessment comparable to the TWIC, they will continue to utilize their existing authority to board regulated vessels and enter regulated facilities as needed for official business and should continue to be afforded access in accordance with existing approved security plans. However, we encourage local and State officials to obtain TWICs to facilitate access to facilities and vessels when such access is a regular part of their duties.

Regarding the status of ''port police'' who receive the same training and certification as local or State law enforcement officers being exempt from the requirement to obtain a TWIC, we disagree with the commenter. These individuals can be exempt only if they are actual State or local officials due to their employment status and statutory law enforcement authority.

Other commenters requested clarification of the applicability of the requirements of this final rule to emergency first responders other than law enforcement, such as firefighters and emergency paramedics. We recognize that emergency responders are an important part of any port. We have extended the option to obtain a TWIC to them, but the final rule has also been changed to state that emergency responders will not be required to show a TWIC to gain unescorted access to secure areas during emergency situations, such as natural disasters or transportation security incidents. We do recommend that they obtain a TWIC if they require unescorted access during non-emergency situations.

(h). Applicability—Voluntary compliance

Two commenters wanted § 101.514(d) clarified regarding voluntary implementation of a TWIC program. They stated that the definition of a TWIC program is confusing, and asked ''[c]an a voluntary TWIC program be used for badging purposes only, but the vessel or facility owner must still obtain approval of a security plan in order to use the card?'' One commenter wants the agencies to explain the opt-in reference from the NPRM, asking why anyone would opt-in when it carries a mandatory follow-up.

One commenter wants the Coast Guard to insert language into the rule regarding voluntary application of the security plan as opposed to voluntary application of the TWIC program.

As noted above in the discussion to changes to the Coast Guard provisions, this final rule no longer contains provisions allowing for voluntary TWIC programs, therefore it is not necessary to respond to these comments at this time. These provisions have been eliminated due to the fact that neither TSA nor the Coast Guard can, at this time, envision being in a position to approve voluntary compliance before the full TWIC program (*i.e.*, reader requirements) is in place. We will keep it in mind, however, as we develop our NPRM to re-propose reader requirements.

3. Coast Guard Roles

Several commenters expressed concern that the challenge to operators who service multiple ports increases as each COTP is given broad authority to establish and enforce different standards.

We agree that consistency among different COTP zones is important and that different COTP interpretations of a final rule, such as TWIC, can create a challenge especially for those operators who service multiple ports. We also agree that some degree of discretion and flexibility is critical to the successful implementation and enforcement of all Coast Guard regulations throughout a COTP Area of Responsibility. To enhance nationwide consistency of the TWIC regulations, the Coast Guard will continue to create and distribute robust field guidance for use by all COTPs. In most cases, Coast Guard field guidance is available to the public and industry for their own use in preparing for inspections and examinations. Should an operator feel that different interpretations of a particular regulation by two or more COTP are negatively impacting their operation, they are welcomed and encouraged to contact the appropriate Coast Guard District Commander for resolution.

A commenter asked who would enforce the escort requirement and the other TWIC requirements. The Coast Guard will continue to be the primary enforcement authority for all MTSA regulations.

One commenter expressed concern that the Coast Guard has been unable to ascertain and report on the number and types of valid merchant mariner licenses or merchant mariner documents in existence at any time, and that this suggests a limitation in its ability to call

on merchant mariners in response to a national emergency. This comment is addressing the Coast Guard Merchant Mariner Credential (MMC) rulemaking, and so we have not addressed it there.

One commenter requested that the Coast Guard articulate its intentions with regard to production of an identification document complying with the International Labour Organization (ILO) standards for U.S. seafarers.

As the United States is not signatory to the International Labour Organization Seafarers' Identity Document Convention (Revised), 2003 (ILO–185), no plans have been made at this time to produce an identification document complying with that particular standard.

Several commenters suggested that the background checks for TWIC be combined with those required for MMC. Two commenters suggested that TSA perform the security threat assessments for Merchant Mariner Documents (MMDs) as well as TWICs and that the Coast Guard use the results of such assessments in its processing of MMD applications. Others suggested that the consolidated review process should be carried out by Coast Guard.

At this time, the option of having TSA or Coast Guard conduct all the required background checks for individuals who require both the MMCs and the TWIC is not feasible. TSA has established a system and process for ensuring individuals applying for the TWIC undergo a consistent security threat assessment and the Coast Guard already has the authority and process in place for conducting the required safety and suitability checks for mariners prior to issuance of credentials. To create a unique system of background checks for approximately one fifth of the expected initial TWIC population would create the need for additional infrastructure within one agency and raise costs for the government and the entire TWIC population. In addition, the Coast Guard has more expertise and authority over the merchant marine than TSA and is in a much better position to determine whether an applicant is safe and suitable to serve in the merchant marine at the rate or rating sought. At this time, the most efficient and cost effective method available for issuing TWICs to credentialed mariners is to have TSA conduct the security threat assessment and issue the identity document (TWIC) while the Coast Guard continues to issue the mariner's qualification document (MMD/License/MMC).

In addition, requiring only one criminal record review for both security and safety-related crimes by one agency would negatively impact mariner flexibility. If only one background check were to occur, mariners would be required to apply for their MMC only at the time they applied for their TWIC. As currently proposed, the MMC and TWIC expiration dates need not align. This allows an individual who works at a port to decide later that he or she wants to become a merchant mariner. In addition, for those mariners who already hold a MMD, License or Certificate of Registry (COR), they need not renew their credential upon the initial issuance of their TWIC, because the effective period of their current credential is not affected by this proposed regulation. If we were to require only one background check by TSA for all mariners, the mariner credential would have to come into line with the expiration date of the TWIC. Requiring mariners who already hold credentials to renew so that their credential's expiration date matches their TWIC expiration date is currently impossible from a legal standpoint due to the statutory requirement that Licenses and MMDs must have a 5 year validity period under 46 U.S.C. 7106 and 46 U.S.C. 7302. Such a requirement would inherently shorten that 5 year duration. Finally, requiring only one security/safety/suitability criminal record review by TSA at the time of application would affect individuals who would like to seek raises in grade or new endorsements on their MMC during the 5 year validity period.

One commenter expressed concern about unanticipated impediments to international transportation resulting from TWIC, particularly regarding rail transportation. This commenter urged Coast Guard and TSA to be prepared to respond quickly to interpret the new regulations and address other unanticipated issues.

We agree that both TSA and Coast Guard should be prepared to make modifications to the TWIC program if needed; any amendments will follow existing requirements for changes to published regulations.

One commenter expressed a desire for standardization of the application process for TWIC or MMD across all regions of the country.

We agree that a standard application process for TWIC and MMD (to be replaced by the MMC) is desirable and a reasonable goal. It is our expectation that all forms, instructions and data collection and processing procedures will be standardized, but not combined, for the TWIC and MMC. As stated earlier, some degree of flexibility will be necessary for local TSA and Coast Guard authorities to best serve the local operators and customers. For example, TWIC enrollment center locations, hours and days of operation are planned to incorporate local industry input.

4. Owner/Operator Requirements

The proposed rule would have required owners/operators of vessels, facilities, and OCS facilities to ensure that security systems and equipment were installed and maintained, including at least one TWIC reader that would meet the standard incorporated by TSA in 49 CFR 1572.23. The proposed rule would have also required that owners and operators ensure that computer and access control systems and hardware are secure.

Several commenters argued that MTSA only mandates TWICs themselves and does not require TWIC readers and their associated equipment. Other commenters were confused as to whether the proposed rule would allow one TWIC reader for an entire vessel and facility or would require a TWIC reader at all access points to secure areas.

Many commenters said that the requirement to place at least one TWIC reader on every vessel would be costly and would not improve security, particularly on small vessels such as towboats. Some commenters argued that their vessel crews are small and that the presence of any unauthorized individuals would be readily apparent. Several of these commenters requested that the final rule waive the requirement for TWIC readers for passenger vessels.

One commenter stated that TWIC readers should not be required in a ship's interior unless required by the vessel's security plan, because existing vessel security plans already adequately address such security concerns. The commenter argued that the locations of TWIC readers should be dictated by the risk assessment performed for the vessel's security plan.

One commenter requested that the final rule allow one TWIC reader for a facility and the vessels that operate from that facility, as long as the facility's security plan incorporates the vessel operations or the facility and vessels have separate approved security plans. Another commenter said that the use of card readers should be optional for facilities and vessels until experience is gained and best practices are developed within the industry.

One commenter requested that the final rule require that facility operators ensure that all readers deployed are fully functional and operational to ensure that all gates are accessible for truck drivers and other affected personnel to use.

Because the use of readers is not required by this final rule, concerns

related to the value or drawbacks related to requiring readers have been deferred. A more complete discussion of why recordkeeping requirements are no longer included may be found below in the section discussing recordkeeping requirements.

One commenter said that § 105.200(b)(8) requirements for adequate coordination of security issues between the facility and vessels that call on it are problematic for both passenger facilities and vessels. The commenter asked that the subparagraph be modified to reference only those that access secure or restricted areas, not the entire facility.

The referenced paragraph, while redesignated, was unmodified by the NPRM or this final rule and, therefore, no changes to the provision were considered.

One commenter said that the proposed rule does not adequately address a facility's responsibility to log seafarers off the ship and onto the facility for routine ship operations. The association asserted that the ship and its crew, by virtue of its clearance by Federal officials to enter port and begin cargo or passenger operations, should be considered a part of the facility and logging off the ship should not be necessary for either normal ship operations or access for shore leave.

Because the recordkeeping requirements have been removed from this rule, there are no specific TWIC logging off requirements. Removal of the TWIC recordkeeping requirements is discussed below.

One commenter stated that the rule must clarify that the owner/operator cannot be held responsible for events rendering employees ineligible for a TWIC of which the owner/operator has no direct knowledge.

Section 105.200(b)(14) establishes a responsibility on the part of the owner/operator to inform TSA of any information that he/she becomes aware of in the normal course of its operations or simply by chance. Whether the information is known ''directly'' or ''indirectly,'' the intent is to ensure that facts, which would affect an individual's eligibility to possess a TWIC, are made available to TSA. The section does not impose a responsibility for an owner/operator to actively seek information on employees or other workers; merely to provide it to TSA should the owner/operator become aware of such information.

One commenter asserted that there is no discussion in the NPRM regarding how owners/operators should deal with a failure in the TWIC system other than to state that they must incorporate backup processes into their plans. The commenter said that TSA and Coast Guard should provide some recommended alternatives. Another commenter expressed an interest in having consistency in the backup processes used by ports and urged TSA and Coast Guard to be more prescriptive on this matter.

One commenter noted the NPRM stated that if the TWIC reader breaks, security personnel should know how to compare the picture on the TWIC with the person's face or have someone vouch for that individual. The commenter then asked if matching a person's face to his or her picture is an acceptable approach to screening, why that method of screening is not an acceptable alternative to the readers more generally. Two commenters said that they supported the inclusion of language that allows operators to include protocols for responding to TWIC holders who cannot electronically verify a match between themselves and the information stored in the cards.

Because the reader requirement has been removed from this final rule, we believe that further discussion of what would constitute acceptable alternate security procedures should the TWIC system fail would be better addressed during a subsequent rulemaking that implements a reader requirement.

5. Requirements for Security Officers and Personnel

One commenter said that he would not have the time to attend any required training to become familiar with the TWIC program.

It is the responsibility of each individual to ensure that he or she receives all the training necessary to successfully perform his or her assigned duties. However, we will work closely with industry and other appropriate stakeholders to ensure that the knowledge requirements can be satisfied by all affected personnel.

One commenter stated that changes to §§ 105.205, 105.210, and 105.215 seem unnecessary because the proposed rule requires possession of a TWIC for unescorted access to a secure area.

We disagree; the provisions provide clarity and avoid any question as to the responsibility of Company Security Officers (CSOs) and other security personnel to have and maintain a valid TWIC.

One commenter asked whether the citizenship of a CSO would affect his or her ability to receive a TWIC. The commenter also asked whether the CSO and other security personnel of a foreign-flagged vessel would need to obtain a TWIC.

Foreign-flagged vessels, including cruise ships, and their crews are exempt from the TWIC provisions, as set forth in 33 CFR part 104. If the CSO is not a U.S. national or legally authorized to work in the United States, he/she may be eligible for a TWIC depending on whether he/she has applied for and received certain types of U.S. visas. We have expanded the eligibility for persons working under valid work visas to open TWIC eligibility to as many of these individuals as possible.

One commenter said that the proposed rule should be amended to provide the CSO with the authority to implement acceptable alternative screening measures for unescorted access to a vessel when the use of TWICs is impractical, unreasonable, and vessel security is not compromised. In particular, the commenter requested that the CSO be empowered with the discretionary authority to modify or exempt TWIC-controlled unescorted access and use the currently accepted procedure of a positive photo-identification along with verification from the worker's company.

Alternative Security Programs (ASPs), proposed and implemented pursuant to the existing regulations, will be available to owners/operators. The ASP must be approved pursuant to 33 CFR 101.120. We do not agree, however, with the proposal to allow CSOs the authority to accept alternative measures to TWIC without first obtaining approval for such an alternative from the Coast Guard. Provisions for seeking waivers or equivalents remain unchanged, and are listed in §§ 104.130 and 104.135, respectively.

One commenter noted that page 29403 of the NPRM refers to the ''access control administrator of the vessel or facility.'' The commenter said that it already has a CSO, FSOs, and VSOs. It asked whether the NPRM would require companies to create a new position or assign a new set of duties to a company employee.

The term ''access control administrator'' was not intended to, nor does it, create a new position. It was used to describe a position that may or may not already exist at a vessel or facility. Additional duties to CSO, FSO and VSO are expressly set out in the Rule, and are not intended to overburden any of those positions.

One commenter asked how much knowledge of and training on the relevant aspects of the TWIC Program VSOs and other personnel of foreign-flagged vessels would be required to have.

Foreign-flagged vessels and their crews are exempt from the TWIC

provisions, as set forth in 33 CFR part 104. VSOs on U.S.-flagged vessels will need to know of those aspects of the vessel's TWIC Program that are relevant to his/her job. For example, if the VSO will be responsible for visually inspecting TWICs, he/she must be familiar with the security features of the TWIC, the alternative procedures to be followed when an individual tries to enter after reporting a TWIC as lost, damaged, or stolen, the procedures to be followed when a fraudulent (altered) TWIC is discovered, and the procedures to be followed when an individual without a TWIC tries to enter a secure area without escort.

One commenter noted that the NPRM proposed requiring that all individuals with security duties and those who may be examining TWICs at access control points have some familiarity with the security features of the TWIC. The company said that TSA or Coast Guard should provide an online course about the security features of the TWIC that can be completed prior to going to the enrollment center, at a kiosk, or at the enrollment center. Successful completion of that course would be required prior to the TWIC application being accepted. Another commenter suggested that the Federal government should provide more extensive outreach and direction to operators and Security Officers prior to finalizing the rule. The purpose of the outreach would be to receive input and to more fully discuss expectations of those who will be given new responsibilities by the rule.

We agree that further guidance on how to fulfill the training requirements contained in this final rule is necessary. The use of online courses may be implemented at a future date. In the interim, further guidance will be forthcoming through publication of an NVIC.

One commenter suggested that the CSO be provided with the option of activating TWICs on behalf of the enrollment centers. We are not considering this option currently, because it may introduce privacy and security issues with the security goals of the TWIC program. However, as the program develops, we will continue to consider ways to allow for greater flexibility in all levels of the program whenever appropriate.

6. Recordkeeping/Tracking Persons on Vessels/Security Incident Procedures

Sections 104.235, 105.225, and 106.230 of the NPRM proposed requiring Security Officers to maintain records for two years of all individuals who are granted access to the secure areas of a vessel, facility, or OCS facility. Numerous commenters, including the SBA Office of Advocacy stated that, in general, the requirement is overly burdensome and would have no resulting security benefit. Several commenters requested a clear understanding of what this information will be used for and justification for the creation and maintenance of each of these records. A few commenters stated that this requirement is overly burdensome on cruise operators because of the volume of people coming and going. One commenter said that this requirement is especially burdensome on operators of small passenger vessels like water taxis but did not state why. Some commenters specifically asked that the requirement be deleted from the rule. Many commenters stated that two years is too long to maintain such records. In contrast, one commenter supported the two-year timeframe.

Many commenters noted that businesses that maintain security videotapes typically keep them for only a brief period. These commenters said that if no security incident has occurred relating to a particular entry to a secure area, there is no need to keep a record of the person involved. Should the Federal government need to ''track'' the presence of employees on vessels, it can obtain and rely on payroll records and other employee files typically kept in the course of business rather than imposing a mammoth new recordkeeping requirement?

Two commenters said that the recordkeeping requirement would further delay the processing of individuals in and out of port facilities, which would affect the flow of freight through the facilities. Five commenters said that the need to keep and access records would greatly increase operating costs.

One association noted that the requirement would force facilities and vessels to install both an entrance and an exit system and said that there have been technological problems with exit systems. It said that exit system technology should be tested before a requirement to use them is promulgated.

Two commenters said it is not clear by whom and where the access records would need to be kept for two years. One commenter suggested that the recordkeeping requirement would make more sense if it applied only to individuals picking up hazardous materials from their facility. A few commenters suggested that the rule be amended to allow video recording to meet the recordkeeping requirement. Additional commenters wanted crewmembers to be exempted from these general provisions to save on paperwork, suggesting instead that crewmembers be logged into the system upon entry to the vessel and logged off upon final exit from the vessel without registering every entry and exit in-between.

Two commenters wanted vendor/contractor personnel to be entered into the database upon initial boarding and then entered again after his final departure. The commenters also stated that there is no need to record every trip made to and from delivery vehicles or shoreside offices/workshops.

Several commenters complained about the lack of personnel to maintain these records. They asserted that facilities will be required to manually enter information on visitors who are exempt from the TWIC requirement. Some commenters felt this was not practical. Two commenters wanted provisions added to the regulation to allow modified procedures for large work gangs, such as longshore gangs vetted by the port, to board the vessel to work cargo without each individual longshoreman being screened by the vessel prior to and at the conclusion of the workday.

Commenters balked at the amount of records that will need to be kept. Two commenters suggested that, to alleviate burden, the records should be automated through the TWIC system, which could keep track of all persons granted access to secure areas. This could be done through an additional access card. One commenter complained that the cost of readers is an unnecessary expense and does not need to be incurred for one-vessel or two-vessel operations, but that without the reader, the paperwork requirements become even more daunting. One commenter wanted the rule to specify exactly what information should be maintained and suggested: Name, ID number, and home address.

As noted above in the discussion of changes to the Coast Guard provisions, the recordkeeping requirements related to TWIC implementation have been removed from the final rule. We had proposed the requirements because we believed they could be satisfied by using the TWIC readers, which were also proposed. Due to our decision to remove the reader requirements from this final rule, it makes sense to also remove the recordkeeping requirements that were intrinsically tied to those readers. We will keep these comments in mind as we consider whether to re-propose new recordkeeping requirements.

Several commenters wrote in opposition to the requirement that vessel or facility owners ensure that

appropriate personnel know who is on the facility at all times.

One commenter said that the requirement would place a tremendous strain on many ports and would provide little value if individuals are properly screened during the entry process. According to the commenter, even if card readers are installed at each entry and exit point and all TWIC holders were to utilize them, provisions would still have to be made to capture data from visitors, vessel crew members, and passengers in freight trucks. The commenter noted that current Coast Guard regulations require ports to grant access to crew members of vessels, including foreign nationals. Because foreign nationals would not be eligible to obtain a TWIC, the port authority said it would have to hire additional security guards to escort crew members while they transit port property. The commenter added that the NPRM had not explained or justified the benefits of knowing precisely who is on a vessel or at a facility at all times or in requiring individuals to use a TWIC to exit.

Another commenter said the requirement would require readers at both entrance and exit gates and argued that exit control is costly and provides little additional protection. The commenter added that other industries have reported technological problems with exit systems. It noted that exit control is not required in the ''higher risk'' aviation sector.

One commenter said that it is not critically important to national security that facilities know exactly who is on a facility at any given time. It is only important to know that everyone on the facility has been cleared to enter. Another commenter said that this requirement would require every facility to construct a security building at every entrance and deploy security guards around the clock. The commenter said that the resulting compliance costs would be prohibitively expensive but would not improve the security of ports because facility operators are already guarding areas determined to be at risk.

Some commenters opposed the application of this requirement to passenger vessels. Two commenters said that because large cruise ships have hundreds of properly authorized visitors onboard at any given time, it would be unreasonable to require a single crew member to know who is onboard. They suggested that the ship's visitor and crew logs be utilized for this purpose because all cruise ships record the arrival and departure of each person while in port. A third commenter noted that passenger vessels can carry thousands of passengers and requested that this requirement be drafted or explained in a way that could ''reasonably'' be applied to passenger vessel operations.

Another commenter recommended that owners or operators be required to know the whereabouts of contractors and visitors, but not facility employees. The commenter stated that it would be extraordinarily difficult to know who is present at a large facility with thousands of employees, because many people ''badge in,'' but not out. The commenter said that the requirement as proposed could require new equipment at multiple access points with little enhancement of security.

Because the use of readers is not required by this final rule, these record keeping requirements and the requirement to know who is on a vessel or facility at all times have also been removed. Comments and concerns on these issues, however, will be considered in any subsequent rule which imposes a reader requirement.

One commenter requested that § 104.290(a)(1) and 105.280(f) be modified to conform to § 104.235 and 105.225, respectively, by requiring the availability of a list of persons who have been allowed access to secure areas, not to the entire vessel or facility.

Because the proposed record keeping requirements have also been removed, we have also removed the requirement that these records be made available after a security incident. Comments and concerns on these issues, however, will be considered in any subsequent rule which imposes a reader requirement.

7. Reader Requirements/Biometric Verification/TWIC Validation Procedures

We received a substantial number of comments on technology issues, almost all of which expressed concern about the feasibility and appropriateness of the proposed TWIC system. Commenters noted that the prototype did not test many parts of the proposed system including the readers and communications with a central database. Some questioned whether the central database is available. They questioned whether the systems will be compatible with existing systems; if they are not the cost of replacement will be high. Commenters stated that TSA must test the proposed system before requiring its use and ensure that it will work in the marine environment and that backup systems will function as well. They stated that if comprehensive testing is not done the result could be higher costs throughout the entire supply chain. In terms of interconnectivity, they stated that the system has to be shown capable of processing 700,000 TWICs instantaneously. Commenters also noted that the system does not appear to have been tested with passenger vessels.

Many commenters stated that cards that had to be inserted into a reader would not work in the marine environment. These commenters stated that TSA had failed to demonstrate the contact readers would work reliably in the marine environment and had not accounted for the cost of frequent maintenance and replacement or the costs imposed by failures that delayed workers and cargo. One commenter noted that when it tested readers outdoors the device did not last five days. Many commenters recommended a contactless reader system as an alternative. They noted that this type of card was used in prototype. Commenters suggested that readers and cards should have mean time between failure of 10,000 hours and at least 6 months between maintenance.

Commenters stated that they needed to know what types of readers would be required before they could be reasonably asked to comment on the rule.

Many commenters questioned whether cost-effective fingerprint readers would work in the marine environment. They noted that the readers require clean screens and clean hands; the latter may be difficult in the marine and port environment. One commenter stated that one member using a biometric reader had a 300 percent annual repair rate, which meant that multiple backup systems will be needed.

Commenters stated that failure rates of 10 percent would have a serious effect on the ability to move cargo into and out of ports. One commenter noted that a failure rate of 10 percent would mean that 3,500 individuals a day would be delayed at LA/Long Beach. If 10 percent of trucks were delayed, the delay would ripple through the entire line of trucks waiting and through the supply chain. They recommended that an error rate must be less than one percent before the system is adopted. Commenters who had implemented biometric readers indicated that they had failed to perform satisfactorily.

After reviewing these comments, we have determined that implementing reader requirements as envisioned in the NPRM would not be prudent at this time. As such, we have removed the reader requirements from the final rule, and will be issuing a subsequent NPRM to address these requirements, instead requiring that the TWIC be used as a visual identity badge at MTSA-regulated

vessels and facilities. That NPRM will address many of the comments and concerns regarding technology that were raised in the above-summarized comments.

Many commenters opposed the requirement to install a TWIC reader on each vessel. One reason for this opposition was that crews on some vessels are small and very familiar with one another, making it difficult for an unauthorized individual to go unrecognized. Other commenters cited the high cost of installing readers on each vessel. Some commenters said that the readers would be difficult to mount on small vessels or would break down in the marine environment. Commenters also said that there is no legislative mandate to require TWIC readers on vessels. Some commenters suggested that the TWICs of vessel crew members could be scanned at the entry point to a facility prior to boarding a vessel.

One commenter said that alternative methods should be allowed for using the TWIC to vet personnel for access on board vessels without the use of readers. One alternative suggested by the company would be to allow all personnel to check in at a central location such as a company office, have their biometrics confirmed, and then be transported to the vessel via trusted agent. At the same time as personnel are being transported, a confirmed list of vetted personnel could be electronically transmitted to the vessel for confirmation purposes. Another commenter opposed a requirement for a TWIC reader on vessels carrying fewer than 150 passengers. A third commenter said that requiring all terminals, regardless of size and technological expertise, to have electronic readers and supporting IT systems in place and operating properly might further compromise efficient terminal throughput. If the readers and related IT systems don't function properly, they will exacerbate congestion and delays. The commenter said it is therefore essential that all technical and process-related issues are thoroughly ironed out before rules are finalized and the program is implemented.

As stated above, the reader requirements have been removed from this rule; therefore, it is not necessary to respond to these comments at this time. Concerns that remain relevant will be considered during the subsequent rulemaking.

One company said that each TWIC would include data on an individual's employer, which would mean getting a new TWIC after every job change. Because of the high turnover rate of vessel personnel, the number of invalid TWICs would grow quickly.

Workers' eligibility to maintain a TWIC is not tied to his or her employer, and employer information is not included on the TWIC itself. Therefore, when a worker changes employment, TSA need not be notified, and neither the TWIC itself nor the individual's eligibility to hold and maintain a TWIC will be affected.

Some commenters pointed out the possibility that truck back-ups could occur or be made worse in the likely event that a truck driver arrives at a reader and finds that he or she does not have their TWIC or their TWIC is inoperable due to being damaged or some breakdown of the system. Another commenter expressed a similar concern about operational delays that could result from lost or damaged cards or system malfunctions during the typical rush of longshoremen arriving for work at or near the same time.

The removal of the reader requirements from this final rule should eliminate the concerns expressed above. Additionally, we have added specific provisions to accommodate persons who have reported their TWICs as lost, damaged, or stolen, to provide continued access for a limited time, until they are able to pick up their replacement TWIC.

Several commenters said that the requirement to check TWICs against an updated list from TSA would be overly burdensome, especially if the list of invalid TWICs becomes large. One company preferred that TSA establish a toll-free number and a website for checking the validity of a TWIC instead of requiring company to maintain a potentially large database. Another commenter said that TSA and Coast Guard should reduce the frequency of TWIC verification at MARSEC Levels 1 and 2. Alternatively, the commenter suggested that a company could maintain possession of a person's TWIC and verify them as frequently as necessary.

One commenter said that TSA and Coast Guard should be responsible to develop a system with which owners/operators can contact TSA to verify the validity of TWICs. The association said that one possible solution is to establish a web portal where facility operators, through a password protected system, are able to match a name and picture with the TWIC ID number.

Many commenters said that most vessels do not have Internet access and therefore would have trouble regularly updating their list of valid TWICs by downloading data from TSA. One commenter said it would theoretically be possible to employ an agent at each port of call to physically deliver downloads to a vessel, but this would significantly increase the cost of the program. Another commenter noted that not all marine employers have computers, so there must be a way (*e.g.*, telephone-based system) for those without computers to check the validity of a TWIC.

One commenter noted that there are a number of areas on western rivers that are wireless dead zones. The company also noted that few existing vessels have satellite Internet connection capability and any such expectation should be included in the economic analysis. The commenter also added that if TSA and Coast Guard expect vessels to use landline connectivity, the cost to stop a vessel periodically (weekly or daily) to download the latest information to vessel card readers would be significant and should be included in the economic analysis.

Two commenters questioned whether satellite communications would remain available for civilian use at elevated security levels. One commenter said that at MARSEC 3, the Federal government takes control over communications satellites, thus making it impossible to download any data from TSA via satellite.

Several commenters said the proposed frequency for updating the TSA information used for TWIC screening is excessive. Several suggested alternative update frequencies for each MARSEC Level. Two commenters said the proposed update frequencies should be the same as for validation of HMEs (annually). A company involved in responses to marine spills said that the requirement to update its list of valid TWICs would be cumbersome and an extra burden during responses.

One commenter suggested that information about individuals who are determined to be a security risk should be communicated to the local Coast Guard for immediate dissemination to FSOs. The company argued that it would be ''ridiculous'' to require a time-sensitive industry to employ computers to search through millions of names in a national database to identify a name not on the list. The company said that national security would be better served by providing the much shorter list of ''non-authorized'' persons. One commenter requested that the rule clarify that a private regional entity under contract to a terminal operator would be allowed to maintain the database of valid TWICs for the operator.

Although a reader is not strictly necessary for checking the validity of a TWIC, in most cases, we believe that requiring facilities to manually check the validity of TWICs without including reader requirements is impracticable. Therefore, because the reader requirement has been removed from this rulemaking; the requirement that the credential's validity be checked against the TSA list of revoked credentials also has been removed. The Coast Guard, when conducting spot checks, will verify a TWIC's validity while confirming the identity of the TWIC holder. We will continue to consider ways to provide flexibility to owners/operators in satisfying this requirement in subsequent rulemakings.

One company asserted that TSA and Coast Guard had not provided any information to the regulated community regarding the size or format of the data files likely to be associated with the list of invalid TWICs. Without this information, the company said it could not provide detailed comments regarding the cost or difficulty in providing this information to its vessels or whether it is even possible with the systems currently in place.

We agree that this type of information is necessary for industry to effectively implement these requirements, and will keep this comment in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

One commenter said that U.S. vessels face connectivity issues when transiting foreign ports and would therefore not be able to comply with the proposed requirement.

We will keep this comment in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Another commenter suggested that facial recognition should be allowed at MARSEC Level 1 instead of biometric verification. Another commenter asked what facilities would be required to do if there are delays in updating its database. The commenter said that this is a critical point, because many other high-priority actions would be taking place at MARSEC Levels 2 and 3.

These requirements have been removed from this rule and therefore, concerns related to the use of the credential at different MARSEC levels will be revisited in a subsequent rulemaking.

A commenter said that rather than placing the burden on employers to repeatedly check the validity of each worker's TWIC, the vessel or facility operator should have the option of registering its employees and others who access its vessels or facilities using a TWIC with the Coast Guard. The Coast Guard would be responsible for notifying the operator if a TWIC it has registered has been invalidated.

As set forth in the NPRM, owner/operators could register its employee and others who access its vessel or facility using a TWIC with TSA, and TSA would notify the owner/operator if a TWIC is subsequently invalidated. TSA describes the process as ''privilege granting.'' This process will still be available, even though we are not requiring owners/operators to routinely validate TWICs in this final rule.

One commenter questioned whether the Federal government would be able to update the list of invalid TWICs on a daily basis at elevated MARSEC Levels. Another commenter conjectured that if there is a terrorist incident that leads to elevated security measures, Internet and other communications systems would likely be taxed to the point of failure. This would make frequent updates of the TWIC database difficult if not impossible.

While it is impossible to predict with certainty how essential infrastructure will be impacted by a terrorist incident, we believe that the layered security approach imposed by the MTSA provides the best approach to ensuring the greatest protection to our maritime facilities. However, because the reader requirement has been removed from this rulemaking, so has the requirement that owners and operators check the credential's validity against the TSA hotlist. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Several commenters said that the required scrutiny of TWICs should not change with the MARSEC Level. Commenters said that the card is designed to be secure and linked to the cardholder by biometric verification, so the security benefits of additional scrutiny would not be worth the effort. One association opposed the requirement that vessels download daily updates on the status of TWICs at MARSEC Levels 2 and 3. The association said that the proposed rule's discussion of MARSEC Levels was not based on reasonable risk analysis. One commenter said that the requirement for use of a PIN and daily check of TWICs at MARSEC Levels 2 and 3 would provide only a marginal increase in security that is not worth the time, effort, and potential problems these measures would create. Another commenter opposed the proposed requirement that all TWIC-enabled gates be manned at MARSEC Level 2, saying it would divert security resources when they are most needed. One commenter said there is no history of legislative intent during the development of MTSA for a requirement that industry download latest TSA information during increased MARSEC Levels.

These requirements have been removed from the final rule and therefore, we defer any response to these comments. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

One commenter maintained that weekly/daily verification for maritime workers was unjustified based on the fact that hazardous materials truck drivers, who pose a greater security threat (due to operation by a single individual and close proximity to population centers and potential terrorist targets), are checked annually.

We believe that this commenter misunderstood what the NPRM meant by the weekly/daily verification, but note that the final rule does not include this verification procedure, and therefore we need not respond to it further at this time.

Some commenters stated that their facilities are not transportation facilities, and as such the cards will be used only to clear employees into the facility. They stated that their existing systems are sufficient and that shifting to the proposed TWIC would double the time required to process each employee, which could cause operational delays during shift changes. The TWIC system should be designed to be easily integrated into legacy systems or TSA should allow facilities to use their existing systems after an employee obtains a TWIC.

The NPRM was drafted to allow owners/operators to continue to use their existing access control systems so long as they were able to integrate the TWIC into those systems. The elimination of the reader, biometric validation, and card verification pieces from this final rule does not change this. In order to integrate the two systems, owners/operators will need to ensure that their own access control systems are updated to show whether the employee has a TWIC even when he/she presents only the facility-specific badge. In other words, an individual must still have a TWIC before he/she can be granted unescorted access to a secure area, even if the badge being used to gain entry on a day-to-day basis is not the TWIC.

The Navy stated that Department of Defense Common Access Cards (DOD CACs) should fulfill the TWIC requirements. As long as the DOD CAC is the official credential for the Navy, it

will meet the identification requirement in § 101.514(b) when required for official duties authorized by the Navy. If it is replaced with another credential in order to gain compliance with HSPD–12, however, that new credential will need to be used by Naval personnel seeking to gain unescorted access to a MTSA-regulated vessel or facility.

8. Access Control Issues

(a). New Hires/Persons Needing Access Before TWIC Is Granted

Many commenters remarked that seasonal workers are employed for 90 days or less, and those commenters believed that the rule would severely impede seasonal hiring if the workers had to wait 60 days for a TWIC. Some commenters pointed out that seasonal businesses often must find new or replacement staff quickly. An association noted that seasonal workers are generally students, who may not know where they are going to work 60 days before classes end. Another association described how a business might not have enough TWIC holders at the beginning of the season to escort the rest of the workforce.

We believe that the inclusion of the ''employee access area,'' discussed above, should operate to exclude the vast majority of seasonal employees from even needing a TWIC.

Some commenters mentioned similar problems with short-term workers and casual labor hired with little advance notice, and those commenters described instances where workers are needed immediately. For example, in some businesses, deckhands come and go at a greater frequency than 30 days. One commenter remarked that it is not uncommon for a new hire to get onboard only to find out that they are not suited for work on vessels, leaving them scrambling to fill a position when a crewmember leaves. A State port authority noted that in addition to new hires, other individuals might need occasional unescorted access without having to wait for a TWIC card.

Several commenters objected to the fact that new hires would not be able to work until they obtained a TWIC card. Many other commenters agreed that the requirement would hurt the ability of companies to hire new workers and mentioned the high turnover rate in the industry, especially among entry-level positions. As one commenter described the situation, ''When a worker needs a job, he or she needs a job now, not 30–60 days from now. If we cannot readily put people to work, there are any number of non-maritime employers who will be happy to hire them and put them to work immediately.'' Commenters added that vessels and facilities would have to add security personnel to escort new hires and that TSA should develop some mechanism, such as temporary access, to address the period before the new hires or existing employees receive their TWIC cards.

One commenter had a suggestion for temporary access for visitors requiring unescorted movement for special cargo deliveries from a transportation mode not usually found in the maritime sector (*e.g.*, oversized loads of equipment being shipped outside of the United States). A temporary TWIC should be established which can be granted by the facility after verifying two forms of identification and a check of databases. Various private companies already offer this service and DOD uses it for contractors and vendors to enter U.S. Army facilities.

Many commenters encouraged TSA and Coast Guard approval of a probationary period during which a new hire could begin work or training while the TWIC application is pending. Such a period could begin after the vessel, facility, or port has conducted its own background checks. Other commenters also favored a simplified or expedited background check (similar to those for firearms purchases) and interim, site-specific authorization for access. Some commenters specifically mentioned a temporary credential, similar to a temporary security clearance, or a pass authorized by the vessel or FSO. One commenter generally favored a shorter duration card.

A few commenters had suggestions about a different security system for short-term workers. One of them emphasized that casual laborers in the maritime industry may work for only one day, but casual laborers often outnumber permanent employees, so the requirement for escorts is impractical. One commenter added that the process required by the regulations must be flexible enough to allow small operators to respond to time sensitive demands for service, and cost-effective enough to allow these same small entities to continue to remain in business. Another commenter wanted to continue with its current photo ID system. A third commenter favored having annual renewal of the TWIC.

After reviewing these comments, we recognized the need to provide owners/operators with the ability to put new hires to work immediately if an urgent staffing requirement exists, once new hires have applied for their TWIC. We have included, above, a detailed discussion of the new provisions that have been added to this final rule to allow new hires to have access to secure areas for up to 30 consecutive days, provided the security threat assessment process has begun, the new employee passes an initial TSA security review, and the individual remains accompanied while in the secure area. In addition, if TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend a new hire's access to secure areas for another 30 days. Additional guidance on this provision will be forthcoming in a NVIC.

(b). Persons With Lost/Stolen/Damaged TWICs

Several commenters expressed concern that key personnel will lose their TWIC and not be able to enter a marine terminal or a vessel until they receive a new one. Several questioned TSA's estimation that replacement cards could be printed and shipped within 24 hours. One noted anecdotal evidence from participants in the Delaware River pilot that nearly two weeks elapsed before a replacement card was ready for activation. Another noted that the 24-hour estimation provided in the NPRM did not account for shipping time or the time required for an applicant to get to a TWIC enrollment center and that 3–4 days may be required for the entire replacement process. Many commenters indicated that it was important to ensure that individuals continue to access appropriate facilities while they await replacement cards or when they simply forget to bring their TWIC with them to work. Failing such access, operators will face burdensome work interruptions and employees might seek a different job or request unemployment compensation.

Commenters offered several suggestions regarding measures to mitigate delays that could result from lost, malfunctioning, or forgotten TWICs: (1) Temporary cards issued while an applicant awaits a replacement card; (2) some type of receipt indicating that the replacement card had been ordered; (3) providing a mechanism for a vessel/facility operator to capture the biometric from the card or from the TSA database for storage in the local database and validate an individual's identity by matching his fingerprint with the biometric stored in the local database in the event the individual leaves his card home on a given day; or (4) alternative identification verification provisions (*e.g.*, visual identification, confirmation call to vendor's employer) included in vessel security plans for situations where mariners and shoreside personnel seeking unescorted access to the vessel have lost or forgotten their TWIC.

As noted above in the discussion to the changes to the Coast Guard provisions of this rule, we have added specific procedures for owners/operators to use to allow individuals to continue to gain unescorted access to secure areas for seven (7) consecutive days in the case of lost, damaged, or stolen TWICs. This procedure should alleviate the concerns over work slow downs or stoppages that were expressed by the commenters above.

One commenter noted a related issue that mariners whose TWIC is lost, stolen, or inoperable may have to be replaced on very short notice and that finding replacement workers could result in operational delays and other problems.

It is likely that the provisions added into the final rule, to allow for individuals with lost, damaged, or stolen TWICs to continue to work for up to seven (7) days, will alleviate this problem.

(c). Use of PIN

Several commenters objected to the requirement for TWICs to have an accompanying PIN number. Many of these commenters said the other security protections in the card would obviate the need for a PIN. In general, comments on this issue reflected two different interpretations of the proposed rule's requirement regarding PIN numbers. Some commenters assumed that the PINs would only be required at elevated security levels, while others assumed that TWIC holders would have to enter the PIN each time to unlock the biometric features of the card. One commenter opined on the treatment of PIN numbers in the FIPS–201–1 standard. According to the commenter, FIPS–201–1 states that the PIN must be validated before the two fingerprints stored on the card can be accessible. In addition, section 6.2.3 of FIPS–201–1 outlines the authentication steps, which indicate PIN validation occurs before biometric reading/validation. If this is correct, then the PIN will always be used since the NPRM proposes biometric validation when entering the secure area of a vessel or facility. Another commenter echoed these comments on the FIPS–201–1 standard and added that the requirement for use of a PIN regardless of threat level is inconsistent with ''the MTSA philosophy.''

Several commenters opposed the use of a PIN only at MARSEC Level 3. They said that because Level 3 occurs so infrequently, TWIC holders would probably forget their PINs. One commenter requested the use of facial comparison instead of a PIN for an alternative means of identification. This commenter said that use of a PIN would compromise the security of the credential. Two commenters said that if PINs are required, there must be a way to check or reset a forgotten PIN within a very short period of time. Other commenters said that the use of a PIN would lead to long delays in access to port facilities and could disrupt the flow of commerce. Two of these commenters requested that the access system not lock out an individual after several unsuccessful attempts to enter his or her PIN, citing the potential resulting disruptions to the flow of commerce. One commenter said that a PIN entry pad will require additional maintenance (due to exposure to the elements) or additional infrastructure to make it immune to the elements (*i.e.*, enclosed boxes, protective barriers to prevent vehicles from contacting the box, etc.).

Because the reader requirement has been removed from this rule, the PIN requirement will not be an issue for routine access controls. We note, however, that the Coast Guard will be conducting spot checks for TWICs, using hand-held readers, and that if an individual is stopped during one of these spot checks, he or she will need to know the PIN in order to unlock the biometric stored on the card and allow for biometric verification. We are sensitive to those commenters who noted that, without daily use of the PIN, individuals will be likely to forget, however, as noted by some of the commenters above, having a card that is compliant with the current technology standard and provides the appropriate level of security and privacy requires the use of a PIN.

(d). Requirement That All Non-TWIC Holders Be Escorted

One commenter expressed concern about the impact of the escort requirement on visitors who do business at ports. The commenter noted that many port facilities may have normal deliveries (*e.g.*, mail, overnight delivery services) or businessmen and women visiting the port, and that ports should be given flexibility on how to handle these visitors. The organization suggested reviewing how the State of Florida handles visitors if it decides not to grant additional flexibility to facilities in the final rule, and said that the final rule should consider different escort requirements at different MARSEC levels.

Another commenter said that the escort provisions would be especially troublesome for small ports because of their limited security personnel. A third commenter expressed concern about the resources that would be required to escort ''one-time-only'' drivers. A fourth commenter recommended that the type of escorting or monitoring required at Certain Dangerous Cargo (CDC) Facilities be based on a vulnerability assessment instead of dictated by standard, noting that additional information on risk could be incorporated from the Maritime Security Risk Assessment Model (MSRAM) or other assessment tools.

As explained elsewhere in this final rule, the term ''escorting'' has been broadly defined to allow flexibility to owner/operators, based on their individual operations, in satisfying the requirement. Further guidance as to how individual owner/operators can satisfy this requirement will be provided in a NVIC. We expect guidance will describe that when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, side-by-side escort. However, outside of restricted areas, such side-by-side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted.

Two commenters noted that many technicians who work on shipboard equipment are not U.S. citizens. They typically work in areas of the ship that would not be considered public access areas and often work at night or when the regular crew is off-duty. The commenters maintained that vessel crews do not have the extra personnel to escort these technicians. One of these commenters requested that the final rule contain a provision for a foreign citizen to have access to vessels if they are approved by the ship's Master or Chief Engineer and recognized as a trusted worker.

We acknowledge that technicians who are non-U.S. citizens or immigrants are an integral part of the maritime industry. Lawful nonimmigrants with unrestricted authorization to work in the United States may apply for a TWIC. In addition, we are amending the immigration standards to permit foreign nationals who are students of a State Maritime Academy or the U.S. Merchant Marine Academy to apply for a TWIC. Also, we are permitting certain aliens in the United States on a restricted work visa to apply for a TWIC. Applicants sponsored by a U.S. company authorized to work on a temporary basis in the United States under an H visa, individuals employed in the United

States on an intra-company transfer under an L visa, NAFTA professionals in the United States under a TN visa, nationals of a country that maintains a treaty of commerce and navigation with the United States and is engaging in substantial trade under an E–1 visa, is in or is coming to the United States to engage in duties of an executive or supervisory character under an E–2 visa, applicants with extraordinary skill in science, business, or art entering the country on an O visa, and Australians in a specialty occupation under an E–3 visa are now authorized to apply for a TWIC. The companies that hire these individuals are required to notify TSA when the workers are no longer employed at their U.S. operations, recover the TWIC, and return it to TSA. In addition, the rule requires the workers to surrender the TWIC to the employer when leaving that place of employment in the United States. We are requiring the surrender and retrieval of the TWIC to prevent instances in which a worker would hold a 5 year TWIC, but be authorized to work in the United States for a much shorter period of time.

One commenter said that the escort requirement, when combined with other requirements in the proposed rule, could have the side effect of completely dismantling what remains of the U.S. Merchant Marine. The commenter said that companies will only flag their ships in the United States as long as there is an economic incentive for them to do so. The commenter maintained that the cost of providing TWIC-carrying escorts for all foreign citizens, purchasing the necessary equipment, and paying for more training could motivate companies to flag their ships under another country's flag.

We share concerns about unintentional negative impacts TWIC implementation could have on the maritime industry. Where the governing statutory provisions provide the Department with discretion, we continue to weigh the security benefits of implementing TWIC against the burden it imposes upon industry. We believe that the provisions set forth in this final rule reflect a reasonable implementation that will not overly burden industry and we will continue to evaluate the impact on industry as we proceed with future rulemakings.

One commenter expressed concern about how maritime ministry activities would be affected by the implementation of the rule.

The Coast Guard supports the activities of those organizations providing services to seafarers of all nationalities. Chaplains and other humanitarian workers are encouraged to obtain TWICs and to work with owner/operators in preserving continued unescorted access to vessels and seafarers.

(e). Vessel-Specific Issues

Coast Guard proposed adding § 104.106 to provide for passenger access areas on board passenger vessels, ferries, and cruise ships, which would allow vessel owners/operators to carve out areas within the secure areas aboard their vessels where passengers are free to move about unescorted. Many commenters supported this provision and stated that these concepts are absolutely essential to a workable rule. The commenters argued that without this provision, the passenger vessel industry, which depends on attracting the public as customers, would not be able to function. Several of the same commenters stated that the clarification that a vessel employee whose duties require unescorted access to a passenger access area, but not to secure areas of the vessel, would not need a TWIC needs to be explicitly stated in the language of the final rule.

Some commenters wanted clarification of the different types of areas on a vessel. One commenter was unable to determine whether all areas not designated passenger access areas are to be considered ''secure areas.'' The commenter noted that, using the definition of passenger access area as found in proposed § 104.106, a passenger area would not necessarily be within the access control area or ''secure area'' of a vessel or facility, which seems to be a contradiction as it is written in the proposed rule.

As defined in § 104.106, passenger access areas are located within the access control areas of the vessel (and are thus within the ''secure area''), but by definition they are not part of the secure area. They can be thought of as pockets within the secure area—all areas around the passenger access areas are secure and require TWICs for unescorted access, but the passenger access area does not. As such, any employees whose duties keep them entirely within the passenger access area do not need a TWIC, the same way that passengers would not.

Some commenters also noted that certain vessel spaces are absolutely essential to security (*i.e.*, the bridge and the engine room), adding that the current MTSA regulations use a definition of ''restricted area'' that implies that only certain portions of a vessel will be so designated.

We agree that only certain portions of the vessel need be designated as restricted areas. As noted above in the discussion of the definition for secure area, we considered requiring TWICs only in these areas, but determined that doing so might actually be more harmful to owners/operators. The NPRM included reader requirements, including the use of the TWIC and readers for biometric verification. Using the restricted area as the secure area would have required that these readers and the verification be used at the entry points of each restricted area. This would have likely meant that many vessel owners/operators would have needed more than one reader, increasing their compliance costs. Additionally, the process of biometric identification could have interfered with the operation of the vessel. As a result, we decided to define the secure area as the access control area, thus limiting the number of readers required, as well as the number of times biometric verification would need to take place.

This final rule does not include the reader and biometric verification requirements, but we do expect to issue a second rulemaking in the future that will re-propose these requirements (although they may have some differences from what was included in the NPRM of May 22, 2006). Because we expect to require readers and biometric verification in the future, we do not think it is a good idea to confuse the maritime industry by adopting a definition of secure area in this final rule that would not be workable when reader requirements go into effect. As such, we did not revise the definition of secure area to coincide with the restricted areas.

One commenter requested clarification that for foreign-flagged cruise ships, the Flag State-approved and ISPS Code compliant Ship Security Plan (SSP) is where passenger access issues would be discussed. The commenter wanted confirmation that no additional plan, such as the TWIC Addendum described in proposed § 104.115, or revision to existing plans is necessary for foreign flag cruise ships under either of these regulations.

For reasons discussed above, § 104.105 exempts all foreign-flagged vessels, including foreign cruise vessels, from TWIC requirements.

Another commenter noted that the creation of § 101.514 does not address the existence of a ''passenger access area'' as an exception, and the language of § 104.100 needs to be referenced here with other exceptions to having a TWIC. Therefore, the commenter suggested that a new subparagraph should be added to read: ''No passenger, employee, or other individual needs to possess a TWIC to

obtain unescorted access to a passenger access area as defined in § 101.106 or a public access area as defined in § 105.106.''

We do not agree with the suggested change. Because the definition of passenger access area clearly states that these areas are not secure areas, it is clear that TWIC requirements do not apply within the passenger access area.

One commenter stated that contractor personnel working for oil and gas operators on vessels would be required to carry a TWIC or be escorted on the vessel. The commenter concluded that, with up to 36 oil field workers on a vessel, this would put a strain on the crew to escort the individuals without a TWIC.

This is technically correct, however we hope that the clarification of what was meant by ''escorting'' will alleviate these concerns and any additional strain on vessel crews. In our clarification, we expect that when in an area defined as a restricted area in a vessel security plan, escorting will mean a live, side-by-side escort. However, outside of restricted areas, such side-by-side escorting is not necessary, so long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be found in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted.

One commenter noted that the proposed rule does not address how to handle access control and identification on vessels under repair in shipyards or in drydock. The commenter suggested that the rules should specifically address this issue and state that the owner of a vessel that is withdrawn from navigation, whether permanently or temporarily, is not required to implement or maintain access control and identification requirements while the vessel is not in navigation.

The MTSA regulations already state that vessels that are laid up or out of service are not subject to part 104. This applies to vessels no longer anticipating MTSA operations. For vessels that are undergoing repairs of a temporary nature, they must be in compliance with their approved VSP including access control measures. However, the approved VSP may contain security measures for intermittent operations, such as drydocking and shipyard repair work. These intermittent security measures may include relaxing access control measures during repair periods, but will include specific measures to reestablish access control and monitoring of the vessel and conducting a sweep of the entire vessel to ensure no unauthorized objects have been left aboard.

Referring to proposed § 104.265(c)(4), one commenter stated that this requirement implies that a MODU vessel with several restricted (secured) areas, would be required to have a card reader at the entrance to each of these areas. The commenter argued that the vessel should only be required to have a card reader at the point(s) of embarkation to the vessel. Additionally, the commenter stated that the vessel would incur undue burden to ensure that a person trained in the TWIC to be assigned/posted at the entrance to each secure area and verify the TWIC for these people.

This comment displays a confusion regarding the meaning of secure area. It is not to be read as meaning the same as restricted area, but rather to coincide with the access control area of the vessel or facility. In the case of a MODU, this would be the entirety of the vessel. Additionally, the MTSA regulations allow for the checking of identification at the point of embarkation to the MODU, and the TWIC provisions do not change this.

One commenter supported proposed § 104.265(c)(8), which permits coordination, where practicable, with identification and TWIC systems in place at facilities used by vessels. The commenter recommended further broadening these provisions to clarify that when a vessel is berthed at a facility which is required under part 105 of these regulations to have a TWIC system in place, the vessel may suspend its TWIC operations while berthed at that facility. The commenter argued that there is simply no need to require duplicate TWIC validation especially when considering that facilities and vessels already have other non-TWIC security and access procedures in place.

We do not agree with this comment; the vessel owner/operator must maintain the ultimate responsibility for the security of his or her vessel. Amending the regulations as the commenter suggests would shift that ultimate responsibility to the facility owner/operator without requiring a contractual relationship with the vessel, which is inappropriate.

(f). Facility-Specific Issues

A law firm representing six companies suggested the following technical change to § 105.255(a)(4): ''change the word ''Prevent'' to ''Deter'' to be consistent with the rest of the maritime security regulations.''

We disagree with this recommendation. Owners/operators must ensure the implementation of security measures to prevent an unescorted individual from entering an area of the facility that is designated a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

The same law firm requested a clarification of § 105.255(d), asking ''what is the meaning of the phrase 'complies and is coordinated with TWIC provisions.'''

This provision allows the facility owner or operator to use a separate identification system, but it must be in addition to the TWIC. Requiring coordination means that the separate ID system cannot be used if it would allow someone without a TWIC to get unescorted access to secure areas.

We received one comment on the requirement proposed in § 105.255(c) (3) for facility operators to ensure that the facility operator's TWIC program ''uses disciplinary measures to prevent fraud and abuse.'' The commenter stated that this would not be the correct assignment of responsibility, because the relevant evidence is only in the possession of government. The commenter also stated that the TWIC is a federally-issued credential obtained by an individual without the involvement of a facility operator or employer. If a TWIC is fraudulently obtained and used or abused in some manner, that would be a serious matter to be addressed by Federal law enforcement and not a subject for employer-imposed discipline. The commenter contended that the employer would not have the necessary evidence to impose discipline under the regulations.

The existing regulations already required owners and operators to have disciplinary systems in place to enhance the legitimacy of their identification system, whether it was a facility issued badge or a State-issued identification credential. There is a difference as to what the disciplinary system would be in each case, but we do not think it is inappropriate to place this responsibility on the owner/operator. For example, the facility owner or operator could fire and possibly take legal action against someone for tampering with the company's badging system, but if they found someone presenting a suspected fake ID, an appropriate disciplinary measure could be to deny access, and could even go as high as firing the individual. Similar disciplinary measures can be put in place in regards to TWIC.

One commenter noted that § 105.255(f)(4) implies that vessel crew and others seeking access to a vessel via a facility, who do not have a TWIC, fall under the definition of ''any person''

when visiting a facility. The current version of this section, § 105.255 (e)(3), reads ''vessel passengers and crew,'' while the above-proposed wording eliminates the word ''crew'' from the section.

The phrase ''vessel personnel and crew'' was removed and replaced with ''any person'' to clarify that the world of persons without a TWIC who might need access through a facility to a vessel is bigger than just vessel personnel and crew. If, however, the vessel personnel and crew do have a TWIC, they would no longer fall into this category of ''any persons,'' but rather into the separate category of persons with TWICs.

Some commenters argued that the proposed regulations are unclear about whether the currently accepted forms of seafarer identification are considered ''government identification.'' One commenter noted that the Coast Guard's section-by-section analysis to § 105.255 reads that persons presenting for entry who do not hold a TWIC would still be required to show an acceptable form of identification, as set forth in §§ 101.515 and 104.265(e)(3). Current Coast Guard guidance states that passports, seaman's books, STCW endorsements, and driver's licenses are acceptable forms of identification that a foreign mariner could use to access a facility. The commenters proposed that the Coast Guard either add the existing approved documents contained in current Coast Guard guidance to the list of acceptable items in proposed § 105.255(f)(4), or clarify in the comments to the final rule that existing approved documents are still acceptable as ''government identification'' so long as they comply with proposed § 101.515. The commenters also suggest the Coast Guard add ''crew'' or ''crew of a foreign vessel'' into the list of non-TWIC holding personnel referenced in proposed § 105.255(f)(4).

The list of documents found in § 105.255(f)(4) are intended to be used to verify an individual's reason for accessing a facility. The inspection of these documents should be read in conjunction with the general requirement to check an individual's identification by examining an ID meeting the requirements set out in § 101.515. We have not amended either §§ 105.255 or 101.515 to specify that the items listed in the Policy Advisory are adequate, but we have no intention, at this time, of changing that guidance.

One commenter also recommended the revision of 33 CFR 105.255(b)(1) to read ''Each location allowing means of access to designated secure areas on the facility must be addressed.'' The commenter stated that as currently worded, this subparagraph contradicts 33 CFR 101.105, 33 CFR 105.225(b)(9) and 33 CFR 105.255(a)(4), subparagraph (c)(1), and could be misinterpreted as requiring that a facility's access control program cover a much more extensive area than is the intent of the proposed regulations.

This final rule will no longer be adding language to this paragraph, therefore the suggested change is no longer necessary.

One commenter noted that at small ports, it is the terminal operator's responsibility to ensure compliance with the security plan and that many small ports face a tremendous difficulty in doing the ''people'' side of security. Another commenter stated that port facilities should be given more flexibility regarding escorting of visitors.

We appreciate the concerns raised by the commenters, and have provided clarification elsewhere in this final rule as to what is meant by ''escorting,'' which we hope will alleviate these concerns.

One commenter raised the question of whether family members traveling with truck drivers in the summer would be required to have an escort in secure areas of marine facilities. They pointed out that many truck drivers travel with family members in the summer months.

In accordance with the access control provisions of both the NPRM and the final rule, owners and operators of facilities are required to check identification of all persons prior to granting access and to require a TWIC prior to granting unescorted access to secure areas. In the case of family members traveling with authorized personnel who require unescorted access to secure areas of a facility and also hold a TWIC, it remains the responsibility of the owner or operator to continue to either allow the authorized personnel to serve as the escort for their family member, or to follow the same procedure used for any other visitor that does not hold a TWIC.

Some comments proposed that current security programs or credentialing programs should be evaluated as an alternative to the proposed rule.

The MTSA regulations in 33 CFR parts 101, 104, 105 and 106 provide for acceptance of ASPs, waivers, or equivalents. These provisions still apply, even with the addition of the TWIC requirements. Note, however, that they would only apply to the facility owner/operator's access control responsibilities; they would not alleviate an individual's burden to apply for and obtain a TWIC if they require unescorted access to a secure area.

One commenter said that a universal identification credential such as TWIC, should allow mariners unescorted access to the terminal when there is a valid need for such access, *i.e.*, to reach the job site aboard a ship berthed within the port facility. Indeed, the mandatory provisions of the ISPS Code (ISPS Code—Part A Requirement 16 Port Facility Security Plan) require such facilitation of access by mariners. The commenter stated that owner/operators, in complying with the proposed rule and with approved security plans, should be sufficiently reassured (for liability purposes) to allow unescorted access to the TWIC holders with a legitimate need for admittance, and that the proposed rule should make clear that owners/operators of secure areas who follow their approved security plan and who adhere to the TWIC access control procedures will not be deemed liable for some type of breach unforeseeable within the federal port security regulations.

We agree that possession of a TWIC should serve as evidence that a mariner does not pose a security risk to a facility owner, and that facility owners should be able to rely upon this fact in allowing mariners unescorted access through their facilities in order to facilitate crew changes, take shore leave, or complete a variety of other duties that may require the mariner to step off of the vessel onto the facility. Issues of liability are beyond the scope of this rule.

A commenter expressed concern about how it would implement the proposed rule at its fenced port facilities, where access control is handled by security officers who check the identification of everyone who drives in. The commenter said it did not seem practical to have employees use a card reader just to drive in past the security officers. The company also said that the restricted areas of its facilities are not enclosed spaces that can be locked off, so card readers would not work to control access to them.

While card readers are not required by this rule, owner/operators remain responsible for controlling access to restricted areas in accordance with existing regulations. Additionally, it is noted that the definition of secure area is not the same as restricted area, as explained elsewhere in this final rule. This final rule imposes a responsibility on owner/operators to ensure that only TWIC holders are allowed unescorted access to secure areas. While satisfying the escorting requirement for individuals without a TWIC may be accomplished by other means than

requiring a side-by-side escort in some secure areas, this final rule requires that owner/operators ensure that access to restricted areas by individuals without a TWIC is only allowed while in the presence of at least one TWIC holder.

One commenter said that it is necessary that the rule put the eventual TWIC holding population on notice that they will require a specific, discrete authorization or a ''business purpose'' when seeking access. The company requested that the final rule restore language that is currently in 33 CFR 105.255(e)(3). That language clearly requires that the reason for access be checked as a routine part of access control. The company said that this requirement is an important and essential layer of access security and affirms the requirement in 33 CFR 105.255(a)(4). The company added that this requirement has been muddled and diminished as the requirement for asserting business purpose when seeking access found at 33 CFR 105.255(f)(4) now only applies to persons not holding a TWIC and seeking entry.

Section 105.255(a)(4) clearly establishes the requirement that individuals may only be allowed unescorted access if they: (1) Have a valid TWIC and (2) are authorized to be in the area pursuant to the facility security plan.

(g). Outer Continental Shelf (OCS) Facility-Specific Issues

Some commenters referenced proposed § 101.514, the general requirement that ''all persons requiring unescorted access to secure areas of vessels, facilities and OCS facilities, regulated by parts 104, 105 or 106 of this subchapter must possess a TWIC. . . .'' One commenter stated that this requirement should either be removed from this section and placed individually in parts 104, 105 and 106, or a specific and limited exemption provided for certain vessels regulated under part 104. One commenter said strict adherence to the TWIC requirements is not feasible for off-shore foreign vessels routinely operating on the U.S. OCS. One commenter said § 101.514 is a particularly onerous requirement for newly hired personnel to work on a U.S. flagged mobile offshore drilling units (MODUs) and do not possess a TWIC. Another commenter stated that these limited exemptions should include U.S. flag MODUs and offshore supply vessels (OSVs) because the vessel manning statutes specifically recognize the necessity of permitting these vessels which are operating outside the geographic boundaries of U.S. jurisdiction to employ non-U.S. citizens and immigrants in their crews. The commenter noted that MODUs in particular are often required to employ indigenous labor as a condition of operations on the continental shelf of another nation, and it is difficult to envision a scenario under which these non-citizens could present a security threat to the United States. Similarly, the commenter notes that the manning statutes recognize that non-citizens should be permitted to fill the vacancies created when a vessel sailing foreign is deprived of members of its required complement. The commenter concluded that it is simply unreasonable to expect that an escort with a TWIC can be provided for either a watchstanding member of the crew of an OSV for the duration of a voyage, or to an industrial worker on a MODU for the duration of a foreign drilling contract.

One commenter stated that strict adherence to the TWIC requirements of this part is simply not feasible for vessels routinely operating outside the United States. The commenter argued that application of the requirements, as proposed, would render it impossible to operate a U.S. flag MODU or OSV in foreign waters, would make it impossible to affect repairs in a foreign shipyard, and would negate specific provision of the manning statutes that permit the employment of non-citizens in specific circumstances. Therefore the commenter recommended that the proposed § 104.105(d) be revised to read as follows:

(d) the TWIC requirements, including those related to unescorted access, found in this chapter do not apply to:

(1) foreign vessels;

(2) U.S. vessels employing non-citizen crewmembers under the provisions of 46 U.S.C. 8103(b)(3) or (e), with respect to those crewmembers;

(3) U.S. MODUs, offshore supply vessels or other vessels engaged in support of exploration, exploitation, or production of offshore mineral energy resources operating beyond the water above the Outer Continental Shelf (as that term is defined in section 2(a) of the Outer Continental Shelf Lands Act (43 U.S.C. 1331 (a)).

As noted above in the discussion of the changes to the Coast Guard provisions of this rule, we are adding a provision to the definition of secure area in § 101.105 that states that U.S. vessels operating under the waiver provision in 46 U.S.C. 8103 (b)(3)(A) or (B) have no secure areas.

We are sympathetic to the concerns of OSV owner/operators, whose vessels are required to comply with part 104 but are transporting crew members to MODUs that are not subject to part 106, and therefore will not have TWICs. We believe that the clarification of the term ''escorting'' should provide some relief to these owner/operators.

One commenter noted that the proposed rule states that foreign vessels entering U.S. ports that carry a valid ISPS Code certificate are deemed to be in compliance with part 104, except §§ 104.240, 104.255, 104.292, and 104.295. And, under § 104.105(d), the proposed rule exempts all foreign vessels from the TWIC requirements. Several commenters requested confirmation that the combination of the exemption of foreign vessels from the TWIC requirement and the existing acceptance of ISPS certification for foreign vessels excludes an OCS facility which is a foreign-flag MODU ''on location'' from the TWIC requirements. The commenters also requested confirmation that there would be no TWIC requirements for a non-covered MODU working next to or over a covered OCS facility. Another commenter, seeking clarification of the proposed rule, asked: If you have a voluntary compliance for a MODU and it obtains a flag-issued International Ship and Port Facilities Security Code certificate, is that sufficient for exemption from TWIC requirements?

A foreign-flag MODU ''on location'' in U.S. waters and holding valid ISPS certification would be exempted from the TWIC requirements of parts 104 and 106.

One commenter believed the escort rules were unreasonable for the oil and gas industry and anticipated that these rules would lead to company and service personnel needing to obtain a TWIC.

The clarification to the escort provisions, provided elsewhere in this final rule, should alleviate the concerns of this commenter by limiting the need for live accompaniment to those instances where the company/service personnel are in restricted areas. At all other times, monitoring would be acceptable.

(h). Other Issues

Many commenters said that the rule should give owners/operators of vessels and facilities the ability to use the TWIC as a ''visual identity badge.'' Some commenters specifically advocated visual checks of TWICs at MARSEC Level 1. Another said that TWICs could be used as a visual identity badge in the early stages of implementing the rule and could be used with readers after more experience is gained with the reader technology. One association

asked that passenger vessels and facilities be allowed to employ TWICs as visual identity badges and not be required to install readers.

Several commenters found fault with the statement in the NPRM that ''allowing owners/operators to rely solely on the visual identity badge system is unreasonable in light of the additional cost of the credential, and the available security enhancements that the increased cost represents.'' These commenters did not think the requirement to use TWICS with biometric readers should be justified by the cost of the TWICs themselves. One commenter noted that TSA officials have endorsed the use of a visual identity badge system for airport employees and said that if such a system if sufficient for the aviation sector, it should also be used in the maritime sector. A shipbuilding and ship repair company argued that a visual identity badge system is needed to prevent delays as hundreds of employees arrive for work.

As already noted, this final does not address reader requirements. However, owners and operators may choose to use the TWIC with an existing physical access control system. The hotlist will be available to owners and operators who could use the magnetic strip or the cardholder unique identifier (CHUID) embedded in the credential to tie it into a legacy system that checks those entering against the hotlist. Although this option is available for owners and operators, the use of reader technology is not required at this time. We will revisit concerns related to other uses of the TWIC in the subsequent rulemaking.

Commenters found access control regulations for train workers within the current TWIC proposal unclear. One commenter recommended that rail facilities be allowed to check workers before boarding a port-facility bound train; another was unsure if train operators would require a TWIC and how other rail worker access control issues should be handled by the industry. Similarly, another commenter noted that train crews pose a unique problem because they enter maritime facilities on trains proceeding down the track. Trains do not typically stop at the property line of maritime facilities, and there is no guard house at which the train crews can scan their credentials. The commenter recommended that railroads be permitted to check crews before they get on the train.

Rail workers will require TWICs if their job requires them to have unescorted access to secure areas of maritime facilities. How and when those TWICs are checked is a process for the train operator to work out with the facility owner/operator, in accordance with the latter's FSP, but the baseline requirement is that unescorted access not be granted to secure areas without a TWIC.

Commenters complained that the proposed rule reflects a ''one size fits all'' approach and did not take into account the different levels of risk and vulnerability across the maritime industry. Several commenters said that the proposed rule should be reviewed to assure that is both risk-based and incorporates performance-based standards as much as possible. One commenter noted that most programs implemented under MTSA have thus far relied upon risk-based standards, but that the proposed TWIC rule is based on a ''one size fits all'' formula that applies the same security rules and the same costs to all operators. The association said that the broad application of this approach could prove to be an undue hardship for smaller and less threatened terminals and facilities that do not have access to the same resources as larger facilities. The commenter suggested that TSA and Coast Guard consider whether a risk assessment could be incorporated into the TWIC program, where practical, to minimize any disadvantage or undue adverse impact on smaller marine facilities.

Some commenters noted that the ''Low Consequence Facility'' designation allows the COTP some flexibility in determining how to logically secure the port without burdening industry with unnecessary requirements that produce no viable improvement in terrorism-related security. The commenters asked TSA and Coast Guard to incorporate the ''low consequence facility'' designation into the regulations.

Another commenter similarly requested alternative facility-specific identification systems for ''low-risk operations.'' Another commenter said that a risk/vulnerability assessment would result in more vessels and facilities being exempted from the TWIC requirement. As an example, he suggested that the cut-off for vessels would be between 500 and 5,000 gross tons. Two commenters said that they did not consider the proposed rule to be tailored to specific and realistic security threats facing the inland marine transportation industry. Another commenter said that requiring card readers for low-risk business operations would be unreasonable and unproductive. The company also said that tow operations would be susceptible to armed takeover attempts even with a TWIC requirement in place, so the rule would not provide any security benefits to these operations.

The MTSA regulations are inherently risk-based, as only those facilities and vessels determined to be at risk of a TSI were included in the applicability of subchapter H. The TWIC regulations intended to provide flexibility to owner/operators through the submission and approval process of their individual TWIC Addenda and security plans. Because many of the ''one size fits all'' requirements have been removed from the final rule, we defer a more specific response until our subsequent rulemaking on reader requirements. We will keep these comments in mind as we draft our NPRM re-proposing reader and TWIC validation requirements.

Many commenters said that the proposed rule would cause unreasonable delays for people attempting to enter facilities. Commenters often said that the resulting delays would disrupt or slow the flow of freight through U.S. ports. One commenter referred specifically to employees who move in and out of facilities several times a day. They expressed concern about these employees having to do a biometric verification each time they re-enter the facility. Several commenters said that the delays caused by the proposed rule would result in increased air pollution, because trucks would idle longer while waiting to enter port facilities.

Commenters said that the proposed rule would drive up the cost of goods that are shipped through ports, which would drive business away. One commenter stated that the proposed rule would pose a potentially significant barrier to international trade. Another remarked on the importance of the Port Authority of New York-New Jersey to the regional economy and the need to minimize disruptions to its operations. A commenter predicted that the rule's impacts on port operations would have secondary effects on industries that rely on imports. One commenter said that the cost of complying with the proposed rule would increase the cost of U.S. exports, reducing the competitiveness of American companies in the global marketplace. Another commenter said that the cost of complying with the proposed rule would hurt the competitiveness of U.S.-flagged ships.

The Department understands that this rulemaking imposes costs on businesses. The Department believes that those costs are a product of statutory mandates and the Nation's security needs. We refer readers to the accompanying Final Assessment for further details on our assessments of the costs and benefits of this rule. This

should assuage concerns arising from the use of the TWIC as set forth in the NPRM. We will revisit concerns related to other uses of the TWIC in a subsequent rulemaking.

One commenter requested that the final rule specify that no port facility or vessel may require the visitor or worker to give up possession of their TWIC as a basis for entry. Any handling of the card by anyone other than the cardholder should be limited strictly to the immediate task of processing the card in a reader, and the card must be promptly returned to the holder unless it has expired or been flagged for revocation.

We agree with this comment as it relates to the final rule issued today. We are aware of several facilities that use their own badging system, and as part of that system they require visitors to leave a form of personal identification with a security officer before they are able to receive a facility specific badge. These systems have largely been approved by the Coast Guard. However, we do not think it is appropriate for these visitors to be required to leave their TWIC behind if they have another form of identification they can leave (*e.g.*, drivers license) after the TWIC has been visually inspected.

One commenter said that the original intended purpose of the TWIC was to facilitate access to secure vessels and facilities for those with the right to obtain such access. The commenter said that the original intent did not include denying access to those without a TWIC.

We partially agree. While facilitating access was one intended result, it also had the purpose of increasing security at our nation's ports by identifying those individuals who would receive unescorted access to secure areas. While the regulations do not prevent an owner/operator from granting access to individuals without a TWIC, they are now required to ensure that an individual without a TWIC is either escorted or is not allowed to enter secure areas.

Some commenters said that the rule was written for ''blue water'' ports and oceangoing vessels but would not work well for the off-shore energy sector or the inland towing industry. Other commenters said that the proposed rules appear to have been developed with little appreciation for the operational realities of the American tugboat, towboat and barge industry.

Many of the concerns expressed regarding the TWIC implementation as proposed by the NPRM should be assuaged by deferring TWIC reader requirements to a subsequent rulemaking. We believe that if further flexibility is required in implementation by a particular industry or operation, the waiver and ASP provisions that currently exist in the regulations can provide it.

One commenter recommended that the rule allow facilities to store biometric information from the TWIC in a facility database with the individual's permission. This option, exercised at the discretion of the facility, would allow the facility operator to validate an individual's identity by matching the fingerprint with the biometric information stored in the facility database in the event the individual leaves his or her card at home on a given day. Local controls could be written in the FSP, and approved by the Coast Guard, to prevent abuse of this option.

One commenter wants DHS to grandfather facilities that have installed new access control systems within the last three years so they will recover their costs in implementing them.

Many expressed concerns that the TWIC would displace sophisticated access control systems already in place at regulated facilities. Many suggested that facilities that had invested significant amounts of capital into access control systems be allowed to continue using those systems in conjunction with TWIC. Others suggested that facilities be allowed to use alternate systems in place of TWIC.

TWIC technology can be adapted to existing access control systems, and it was not our intent to force owner/operators with sophisticated systems to abandon those systems to accommodate TWIC. We believe that TWIC enhancements can be fully integrated to most existing physical access control systems, and hope that the language of the final rule clarifies that owner/operators need not replace existing systems so long as TWIC capabilities are appropriately incorporated into the facilities' existing system. A NVIC providing further guidance on applying the access control requirements in this final rule is forthcoming.

9. TWIC Addendum

One commenter said that the time allowed for completion of a TWIC Addendum should be at least one year. The company based this request on the complexity of the proposed program, especially for shipyards that must coordinate TWIC requirements with screening programs required by other federal agencies. Another commenter requested that companies be allowed to submit amendments to their VSPs that incorporate their TWIC provisions rather than a separate addendum. The company said this would mean less work for some companies and for the Marine Safety Center (MSC) that must do the reviews and approvals. Another commenter asked whether the TWIC Addendum would be considered SSI and whether a vessel operator could show the Addendum to people when they come on board the vessel.

One commenter recommended that the Coast Guard be required to notify an entity submitting a TWIC Addendum once the Coast Guard makes a determination of completeness. The commenter said that a confirmation letter from the Coast Guard that a complete submission has been received and is undergoing review would prevent potential delays to vessels that have not yet received an approval letter from the Coast Guard. This commenter also recommended that entities submitting a TWIC Addendum should include a contact point and method by which the Coast Guard could easily accomplish this requirement (*e.g.*, e-mail, fax, or hard copy via surface mail).

One commenter requested that the TWIC Addendum be reviewed by the Coast Guard itself and not by outside consultants.

One commenter said that the requirement that the TWIC Addendum be kept ''on site'' or onboard the vessel should be revised. Specifically, the commenter said that the rule should require the TWIC Addendum to be maintained at the same location as the VSP or ASP. The commenter noted that under one approved ASP, the ASP must be maintained by the Company Security Officer at a secure location, but need not be carried on board the towing vessel. The commenter requested that the same approach be followed with the TWIC Addendum.

One commenter posed several questions regarding how this requirement would apply to OCS facilities (§ 106.115). The company asked if the requirement would apply to a foreign-flag MODU ''on location'' if the vessel has an approved ship security plan (SSP) as required under the ISPS Code. The company also asked how the requirement would apply to a non-self-propelled foreign flag MODU ''on location'' working next to or over an OCS facility that is required to comply with TWIC requirements.

Several commenters stated that Coast Guard should provide clarification on why companies and vessels need to integrate the TWIC Addendum into the ship's security plan. They said that if set up properly, the TWIC Addendum could be a stand-alone document as easy reference for persons with security

duties that are authorized to view this information.

One commenter notes that, as proposed, §§ 105.500 to 105.510 would allow an owner/operator to resubmit an entire security plan with a list of sections amended as the TWIC Addendum, but once approved, it would carry the same expiration date as it had prior to the amendment. He recommended that if the revised plan were submitted to the COPT with a revised facility security assessment, that a new time line should start and the plan should be approved for five years from the date of approval.

One commenter recommended that the TWIC Addendum requirements (33 CFR 105.120, 33 CFR 105.200 and 33 CFR 105.500–510) should be revised to explicitly require facilities to designate the secure area within which access control is required. The commenter stated that once the Coast Guard has approved the TWIC Addendum, the facility would be protected from inspectors voicing their personal opinion that the secure area does not comply with their interpretation of the definition.

We removed the TWIC Addendum requirement from the final rule when we determined that the reader requirements would be delayed until a subsequent rulemaking. The purpose of the TWIC Addendum was to allow the owner/operator to explain how the readers would be incorporated into their overall access control structure, within the standards provided in the NPRM. With the removal of the reader requirements from this final rule, we feel it is appropriate to also remove the TWIC Addendum requirement. In order to ensure that security is not compromised, we have added to the access control provisions in each part (33 CFR parts 104, 105, and 106) to provide specific security measures (as opposed to performance standards) to be implemented by owners/operators in the area of access control. Additionally, because we envision the TWIC Addendum to be a part of the subsequent rulemaking on reader requirements, we felt it would be overly burdensome to also require a TWIC Addendum at this point in time.

As the TWIC Addendum requirement is no longer included in this final rule, we will address these concerns in a subsequent rulemaking.

One commenter said that Coast Guard-approved VSPs should dictate security provisions once an individual is onboard the vessel and that the proposed rule should not establish duplicative security requirements. The commenter said that the VSPs limit access to vessels generally and in particular prohibit access of unauthorized individuals to restricted areas of vessels. The commenter went on to state that TWICs should be used only as a basic identification device and proposed 49 CFR 1572.23 and 33 CFR 104.265 should be amended so that mariners are only subject to the existing VSPs when onboard a vessel.

We disagree that the TWIC establishes duplicative security requirements. The TWIC will enhance existing security requirements by improving the ability of owner/operators to prevent access by unauthorized individuals to restricted areas of the vessel and the vessel in general. Therefore, we decline to adopt the recommendation.

One commenter encouraged the Coast Guard to provide for some flexibility in the drafting of security plans to accommodate port workers who frequently move between secure and non-secure areas during the course of a single operation. The association said that continuous application of the limitation to gain re-entry access would be impractical and could potentially drive up costs unnecessarily. As an example, the association said that they need the ability to service cruise ship vessels without access procedures that require multiple interfacing with biometric readers.

We believe that the use of the TWIC as a visual identity badge, as required in this final rule, will alleviate some of the burden noted in this comment.

One commenter opined on the application of the TWIC requirements to shipyards involved in building and repairing U.S. military and Coast Guard vessels. The commenter stated that these shipyards must already comply with DOD security requirements, and claimed that the security afforded by the MTSA regulations is less comprehensive than the security provided by DOD security measures. The commenter said that complying with both sets of security requirements would be costly and could potentially reduce security by causing confusion and increasing administrative burdens. The commenter noted that the increased costs and administrative delays would be borne ultimately by the U.S. Navy and Coast Guard, and for these reasons requested that the shipyards be exempted from complying with the TWIC rule.

We disagree with this comment as it pertains to ''all shipyards.'' If a shipyard falls within the applicability of the MTSA regulations and is required to submit a FSP under 46 U.S.C. 70105, then any individual requiring unescorted access to a secure area is required to have a TWIC. We note here that shipyards are specifically exempt from 33 CFR part 105 applicability (*see* 33 CFR 105.110(c)), and would only come under the facility security regulations if the shipyard is subject to a separate applicability requirement, such as being regulated under 33 CFR part 154, requirements for facilities transferring oil or hazardous material in bulk.

Both the NPRM and the final rule provide for a means through which security threat assessments done by other governmental agencies may be deemed comparable. If there are background checks in place under the DOD programs, and if those background checks include security threat assessments that are deemed comparable to the one done by TSA, then individuals may receive their TWIC at a reduced cost, but they will still need to apply at a TSA TWIC enrollment center.

Commenters stated that the rule assumes that people with TWICs will be facility employees, but that many are not (particularly truckers).

We disagree with these comments. As we stated in the NPRM, the TWIC requirements applies U.S.-credentialed mariners and to anyone seeking unescorted access to secure areas within MTSA-regulated vessels or facilities. It is not limited to facility employees, nor did we assume it would be.

One commenter noted that FSPs differ based on the threat assessment conducted for each facility. He said that the NPRM might encourage a misunderstanding among the public that every facility is ''doing business'' strictly according to the Code of Federal Regulations (CFR). He said, ''It is very difficult sometime for people to understand that [a facility security plan] may not specifically reflect what the CFR says.''

We do not agree with this comment. If a facility is operating under its approved FSP, then it is in compliance with the regulations. The MTSA regulations are performance standards, and as such there are a variety of ways in which a facility might meet the standards contained therein. Unless a facility has been granted a waiver from portions of the regulations, we fail to see how a FSP would not reflect what is stated in the CFR.

10. Compliance Dates

The NPRM proposed requiring owners/operators to develop and submit TWIC Addendums within six months of publication of the final rule. One commenter pointed out that the Coast Guard allows itself five years to fulfill

its responsibilities, but owners/operators only get 6 months. One commenter wanted the text regarding TWIC Addendum submission to be revised to read ''six months after such date that the Secretary deems the program has been fully implemented within the maritime work force ashore.'' One commenter wanted six months to be extended to at least one year or one year from the time the Coast Guard approves the TWIC Addendum. This would allow time for adjusting capital budgets and integrating the TWIC readers/system with existing access control systems. One commenter wanted to know what happens with regards to this timeframe if TWIC readers are not available when the implementation period begins or are not readily able to be integrated into existing systems.

These sections of the NPRM also would have required vessel, facility, and OCS facility owners/operators be operating according to their approved TWIC Addendum between 12 and 18 months after publication of the final rule, depending on whether enrollment has been completed in the port in which the vessel is operating. One commenter expressed concern that the 750,000 cards needed for initial enrollment cannot be produced within 18 months. Eight commenters believed the timeline is totally unrealistic. One commenter recommended that the ''effective dates'' section be reserved until it is demonstrated that the documents can be issued and equipment is both available and functional, and stated that a subsequent notice could be published in the **Federal Register** establishing effective dates of the access control and credentialing provisions when they are ready. Five commenters requested the deadline be extended. Three commenters wanted to extend the deadline specifically to afford time to budget for TWIC compliance (which typically requires a three-year lead time) and/or request/receive Federal grant funding.

The TWIC Addendum requirements have been removed from this final rule, and as such it is not necessary to respond to them at this time. We will keep them in mind as we draft our NPRM on reader requirements. As noted above, we have also revised the compliance dates slightly. Vessels will now have 20 months from the publication date of this final rule to implement the new TWIC access control provisions. Facilities will still have their compliance date tied to the completion of initial enrollment in the COTP zone where the facility is located. This date will vary, and will be announced for each COTP zone at least 90 days in advance by a Notice published in the **Federal Register**. The latest date by which facilities can expect to be required to comply will be September 25, 2008. Additionally, mariners will not need to hold a TWIC until September 25, 2008. They may rely upon their Coast Guard-issued credential and a photo ID to gain unescorted access to secure areas to any facility that has a compliance date earlier than September 25, 2008.

One commenter stated that the final rule should clearly state the dates for compliance, and found § 104.115(d)(2) to be confusing as written. Two commenters argue that the TWIC enrollment process will never be ''complete'' since employers will always be submitting new applicants for enrollment, and asked who determines that enrollment is complete.

We are sensitive to these comments, however until the contract for the entity that will be operating enrollment centers is complete, we will not know exactly what date will apply to each COTP zone. We will communicate more specific dates as they become available, but can state that we expect that initial enrollment (*i.e.,* the enrollment rollout) will be complete nationally within 18 months of the first TWIC enrollment.

One commenter believed that the schedule for the applicant to provide information is confusing. The implementation schedule in § 1572.19 appears to contradict the schedule in § 104.115.

In order to reduce or eliminate any confusion, we point out that § 1572.19 applies to the individual TWIC holder and § 104.115 applies to vessel owners and operators of regulated vessels.

One commenter said the rule needs to clarify and focus on the Access Control System pilot timeline. Operational tests in selected pilot ports and terminals should be concluded and the TSA data interfaces checked and proven before the Access Control System is designed and the TWIC Addendum created. It is not clear if the timeframes apply to just the TWIC rollout or to both the TWIC and the Access Control System. Three commenters felt that the timeframe could potentially cause significant additional costs to the industry (i.e., obtaining equipment and systems, hiring personnel to run the programs, etc.). Two commenters said the deadline for compliance listed in 49 CFR 1572.19 is unreasonable. It should be extended to a minimum of 18 months from the implementation of the final rule. Six commenters expressed the need for proper field testing of the biometric readers prior to usage. Two commenters were concerned about the logistics of processing applications and issuing TWIC cards to hundreds of thousands of workers. One commenter believed TWIC is being implemented due to political issues and pressures. One commenter thought the timeline should be changed to start compliance after the technology for the cards and the readers has been proven to work instead of the date the final rule is published. Three commenters stated the rule needs clarification between page 29407, where it discusses a phased enrollment process, and page 24909, where it lists timeframes for plans and compliance. They stated that the timeframes do not allow for a phased process. All commenters recommend adopting the phased process, and one added it should be based on risk and employee access to critical infrastructure.

One commenter wanted compliance dates to begin after the Coast Guard has approved the revised plans. Another asked the Coast Guard to review their implementation timeline and ensure that industry has adequate time to successfully implement all of the requirements.

With the removal of many of the more technologically complex portions of the NPRM from this final rule, we have attempted to clarify compliance deadlines for this final rule within the regulation text. The initial enrollment period will be a phased enrollment period, which we estimate will take 18 months to complete. Owners/operators of vessels will be required to comply with the TWIC provisions of this final rule on September 25, 2008. This means that by this date, vessel owners/operators will need to begin visually inspecting TWICs before they grant individuals unescorted access to secure areas. However, many workers on vessels will be required to use a TWIC to access facilities en route to their vessel. Additionally, enrollment center scheduling has been set up to address initial enrollments of merchant mariner and non-merchant mariner workers concurrently at each port. Mariners may apply at any TWIC enrollment center, at any time during the enrollment period. Although mariners are not required to have a TWIC until the end of the enrollment period, they are encouraged to apply early. Vessel owners/operators will be better served ensuring their crews are enrolled during initial enrollment periods because they may need to access many different facilities throughout the country, and facility owner/operators must be in compliance with the access control provisions as the initial roll out enrollment in their COTP zone is completed. As noted above,

these exact dates will be announced in **Federal Register** Notices.

Two commenters requested implementation of TWIC cards be delayed for vessel personnel until the Coast Guard has redesigned its MMC to incorporate TWIC security features or at least 18 months after TWIC reader systems are ready.

With the removal of the TWIC reader requirements from this final rule, this comment is no longer relevant. However, we note that the compliance date of this final rule, for vessel owners/operators, has been changed. Vessel owners/operators need not begin checking for TWICs until 20 months after the publication date of the final rule. Workers on vessels will still be subject to the security procedures at 105 and 106 facilities. Additionally, enrollment center scheduling has been set-up to address initial enrollments concurrently with MMD and non-MMD workers at each port. Vessel personnel will be better served enrolling during initial enrollment periods at each port.

11. General Compliance Issues

One commenter wanted to know how the Coast Guard is going to ensure compliance with the TWIC program. Another cited a need for a means to verify the status of a TWIC in the field and suggested that at a minimum a call center phone number and electronic means are needed. They also suggested an investigation into the costs and benefits of equipping law enforcement personnel with the means to validate driver fingerprints against a TWIC.

At least until we are able to finalize a second rulemaking to impose reader requirements on the maritime community (as appropriate), the cards will be used for access control as visual identity badges instead of being required to be read by an owner or operator's reader at access control points. Additionally, the Coast Guard will be confirming the identity of TWIC holders using hand-held readers, uploaded with the most recent hotlist, during its already existing annual facility and vessel MTSA compliance exams, unannounced facility and vessel spot checks, and for cause as needed. Finally, although the installation of readers is not currently required, the hotlist will be made available to vessel and facility owners and operators should they voluntarily decide to use the credentials within their existing physical access control systems. As an example, an owner or operator could write to the magnetic strip on the card or read the CHUID stored on the chip embedded in the card to tie it into a legacy system that checks the TWIC against the hotlist.

Another commenter wanted to know what protection there is if the facility that you are going to does not comply with the TWIC program.

If the facility does not comply because the MTSA regulations do not apply to it, there is no issue. If however, a MTSA-regulated facility does not visually inspect TWICs as required by this final rule, they are subject to the civil penalty provisions found in 33 CFR 101.415. Anyone who knows of such non-compliance should make a report to the National Response Center (NRC), using the contact information found in 33 CFR 101.305, as such non-compliance is a breach of security.

Two commenters are concerned that TSA and the Coast Guard want to publish a final rule before the end of the year and will not adequately address the numerous uncertainties and questions on this proposed rule that were raised by the commenters.

We disagree with this comment. We have considered each and every comment submitted to the docket during the 45-day comment period, as well as all of the comments received at the four public meetings that were held in late May and early June. We have made several changes to the proposed rule as a result of the issues and concerns raised, the biggest being the delay of the card reader and associated requirements. Additionally, in this ''Discussion of comments and changes,'' we have responded to all of the comments we received.

Four commenters requested that the agencies issue a TWIC NVIC to assure consistent interpretation and application of the program. They also advised that TSA should develop simplified integration plans to assist companies with the implementation.

One commenter suggested that TSA and Coast Guard offer ''best practices'' for industry to use. As an example, the company cited the need for suggestions on handling contractor personnel during major construction projects and plant turnarounds.

We agree that a NVIC will be necessary to assist customers with compliance as well as assure consistency nation-wide; this will be forthcoming to help interpret the provisions of this rule. We are also issuing robust field guidance to all of our COTPs, to ensure uniform application of the requirements.

One commenter expressed concern that union involvement may slow the enrollment process. The commenter wanted to make sure that labor agreements and arrangements are addressed in TWIC.

We do not feel that this final rule is the place to address labor concerns between facilities and unions.

12. Additional Requirements—Cruise Ships

Section 104.295(a)(1) proposed higher burdens on U.S. cruise ships, such as requiring that an individual's identity be checked against their TWIC at each entry to the vessel, and that the validity of the TWIC be verified with TSA at a higher rate than for other vessels. Commenters said that these additional requirements are cost-prohibitive and unfair to owners and operators of U.S.-flagged cruise ships and should be applicable to foreign cruise ships. One commenter opposed this provision, stating that this requirement is excessive, burdensome and does not respond to a demonstrated risk, and under lower MARSEC level requirements, it is not necessary to verify the identity of someone who is a known employee.

While the reader requirements have been removed from this final rule, we do not agree with the comments. Cruise ships do carry a higher risk than other passenger vessels, as the higher number of passengers on-board creates a more attractive target to terrorists. Additionally, the higher number of employees, including licensed crew, entertainers, wait staff, and other unlicensed crew, make it less likely that all employees will be ''known'' to the security personnel checking credentials. However, we will keep these comments in mind as we draft the NPRM to re-propose reader requirements.

Other commenters stated that most procedures for access can be covered under a vessel's security plan. One commenter said the crew was at the heart of the security plan and will ensure vessel security. One commenter suggested that instead of requiring card readers at every vessel entry point, employees should scan their cards at the facility entry point prior to boarding their assigned vessel. Another commenter stated that the proposed rule should be edited to allow for spot-checking of passengers and employee-displayed badges as mandated by a Coast Guard approved VSP at MARSEC Level 1, as current security plan specify.

These comments are no longer applicable, as the final rule does not include the requirements for readers and biometric verification. We will keep them in mind as we draft the NPRM to re-propose reader requirements.

Under proposed § 104.295(a)(2), at MARSEC Level 2, the owner or operator

of a U.S.-flagged cruise ship must ensure that each crewmember or employee seeking to board the vessel is required to enter his or her correct PIN prior to being allowed to board. Several commenters opposed this proposed provision. Another commenter stated that an effective and reliable biometric check is sufficient to verify identity at all MARSEC levels and did not agree that the additional measures of using PIN numbers is necessary. The commenter also noted that most individuals will not remember their PIN number, thus causing unforeseen problems and necessary back-up measures.

Many of these comments are no longer applicable, as the final rule does not include the requirements for readers and biometric verification. We will keep them in mind as we draft the NPRM to re-propose reader requirements.

The comment on the PIN number, however, is still relevant. The cards that will be issued initially and used as a visual identity badge will hold the biometric template on a dual interface chip. The Coast Guard intends to integrate the TWIC requirements into its existing facility and vessel annual MTSA compliance exams, as well as through unannounced security spot checks using hand-held readers. We will monitor issues with PINs during the Coast Guard checks, and if problems are identified, we will address them in the NPRM re-proposing the access control and reader requirements.

13. Additional Requirements—Cruise Ship Terminals

Proposed § 105.290 identified which activities must be done within the facility's secure area, to clarify the identifications to be checked before granting individuals entry to the facility, and to clarify that passengers must be escorted within secure and restricted areas of the facility. One commenter stated that this would require changes difficult to incorporate using an addendum and would require the full FSP to be rewritten. Also, the commenter noted that it is unclear in the proposed rule if ''passenger access areas'' are considered ''secure areas,'' since they would be inside the terminals access control area. The commenter recommended that the regulations be written to allow unescorted passenger access once passengers have passed through the passenger screening locations. One port authority recommended that cruise ship terminal operators be allowed to establish passenger access areas within the terminal, similar to cruise ships. The port authority recommended that this be a defined space within the access control area of the terminal that is open to passengers but does not require a TWIC for unescorted access.

Passenger access areas are not an option for facilities, therefore many of these comments are not applicable. The escorting requirements (as clarified elsewhere in this final rule) for those areas open to passengers within cruise ship facilities should be identical to what these facility owners/operators are already doing under the existing requirements found in §§ 105.275 and 105.290.

Another commenter argued that the regulations should allow cruise ship terminal operators to establish ''passenger access areas'' within the terminal, which would be a defined space within the access control area of the terminal that is open to passengers but does not require a TWIC for unescorted access.

We disagree with this comment. The passenger access area was designed for use by vessels only. Cruise ship terminals should be able to use the security measures implemented to meet the requirements in § 105.290 to meet the definition of ''escorting,'' therefore, we do not think it is necessary to extend the concept of passenger access areas to cruise ship terminals.

14. Additional Requirements—Certain Dangerous Cargo (CDC) Facilities

Section 105.295 proposed making a change to clarify that persons not holding TWICs must be escorted within CDC facilities. All of the commenters on this section stated that this change will be very burdensome for CDC facilities. Several commenters said that any additional necessary measures can be dealt with through the existing regulatory regime. One commenter said any changes should be made on the basis of a vulnerability assessment. Some commenters argued that each FSO should decide whether more stringent TWIC program requirements should be implemented. Another commenter said that any additional security measures should be left to the discretion of the owner, subject to oversight by the Coast Guard through the security plan review and approval process.

We disagree with these comments. Leaving the TWIC requirements in the hands of individual owners/operators, without first providing standards, would create serious security flaws in the TWIC system. However, we are sympathetic to the concerns raised over escorting. As explained elsewhere in this final rule, we did not intend to require a side-by-side escort at all times in all places. So long as the places to be accessed are not parts of any restricted area, the provisions used by the facility to satisfy their monitoring requirements will likely suffice to meet our escorting performance standard.

One commenter stated that since the HME credentialing requirements are equal to TWIC, and HME holders are allowed to transport CDCs, a TWIC holder would not pose a greater security risk than an HME holder. Therefore, the commenter argued that no additional restrictions need to be placed on CDC facilities regarding unescorted access by TWIC holders. The commenter also asked: ''In the case that a CDC facility is a separate location on port real estate (*e.g.*, truck yard close to marine terminals), and it does not fall under the security regulations of Part 105 because it is not a secure maritime facility, what will be the TWIC verification requirements at that CDC facility, if any?''

We agree; under the final rule, all HME holders will be required to obtain a TWIC if they need unescorted access to a MTSA regulated facility. Thus, since all HME holders on a CDC facility would also likely be TWIC holders, they would necessarily be treated the same as other TWIC holders. In answer to the commenter's question, TWIC requirements only apply to facilities regulated under 33 CFR part 105. Thus, if a facility is not regulated by part 105, either because it is not a maritime transportation facility or any other reason, then the TWIC provisions would not apply.

15. Additional Requirements—Barge Fleeting Facilities

Under proposed § 105.296, owners/operators of barge fleeting facilities would take responsibility for ensuring that anyone seeking unescorted access to barges within the fleeting facility hold a TWIC. All of the commenters stated that the additional regulations for conducting access control checks are not practical for this industry. Most of the commenters claimed that these requirements are unnecessary for small facilities and crews, such as those at barge fleeting facilities. One commenter requested that owners/operators of barge fleeting facilities take responsibility for ensuring that anyone seeking access has a TWIC. One commenter requested that the proposed rule accommodate facilities that have plans that allow for use of the card readers at the facility and not on every one of the vessels. One commenter said that the change in the rulemaking to require a TWIC for anybody to access a fleeted barge will effectively raise the competitive pricing for certain services, including

carpenters, electricians, contracted painters, fencing companies, etc.

Because this final rule does not include reader requirements, we will not, at this time, be responding to the comments that addressed reader usage and/or requirements. We will, however, keep them in mind for our future rulemaking to implement reader requirements.

This final rule does still require that barge fleeting facilities ''control access to the barges once tied to the fleeting area by implementing TWIC as described in § 105.255 of this part.'' Section 105.255 requires that TWIC be used a visual identity badge. We do not believe that this should impose an impracticable burden on the fleeting facilities, as they were already required to check identification of persons under the pre-existing MTSA regulations.

16. Miscellaneous

(a). Compliance of TWIC With International Labour Organization (ILO) 185

Five commenters request that TWIC also comply with ILO 185. Two of these also want TWIC to be accepted as an international seafarer identification document. Three of them remarked that the TWIC must be compatible with the ILO 185 in order for the document to be accepted in foreign ports of call. One commenter encouraged the Coast Guard and Transport Canada to enter into a bi-national agreement or MOU to recognize each nation's secured credentials for their respective seafarers (the TWIC for U.S. seafarers and the proposed Seafarer's Identity Document (SID) for Canadian seafarers). The commenter stated that mutual recognition of these documents as equivalent would streamline vessel and marine facility access control procedures and promote easier access to shore leave for seafarers as per the ISPS Code.

As the United States is not signatory to the ILO Seafarers' Identity Document Convention (Revised), 2003 (ILO–185), no plans have been made at this time to recognize the SID as a TWIC equivalent or produce an identification document complying with that particular standard.

(b). Notification of Employer Upon Employee Disqualification

Section 1572.9 (e) states that the applicant must certify the following statement in writing: ''I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified.'' TSA specifically invited comments on this specific requirement. One commenter points out the contradictory requirements between § 1572.9 (e) and the preamble text. The preamble implies that TSA will notify the employer only of the employee's disqualification without releasing the reason for that disqualification. The commenter suggests that TSA include this wording in § 1572.9 (e) in order to protect the privacy of the employee. Another commenter wrote in to support the implementation of this provision.

Consistent with the requirements of the statute, TSA has no intention of providing information to an employer as to why an applicant is disqualified. However, if TSA has reliable information concerning an imminent threat posed by an applicant and providing limited threat information to an employer, facility or vessel operator, or COTP would minimize the risk to the facility, vessel, port, or individuals, TSA would provide such information. We have amended paragraph (e) to clarify this.

(c). Requirement of 46 U.S.C. 70105(b)(2)(D)

One commenter wants to know whether the provisions in 46 U.S.C. 70105(b)(2)(D) were inadvertently left out of the proposed rule or whether they are no longer necessary.

At this time, the Coast Guard has implemented the requirements in 46 U.S.C. 70105(b)(2)(C) and (D) as follows. In this rulemaking, the requirement for all Coast Guard credentialed merchant mariners to hold a TWIC includes all vessel pilots holding a Coast Guard-issued license. We have not extended this requirement to address the issue of non-Federal pilots (those few pilots holding only state commissions or credentials, who do not also hold a federally-issued merchant mariner credential). Also in this rulemaking, we included a requirement that all individuals seeking unescorted access to secure areas of 33 CFR subchapter H regulated vessels must have a TWIC. This population includes all individuals working aboard Subchapter H regulated towing vessels that push, pull or haul alongside tank vessels. We have not, however, extended this requirement to address the issue of all individuals working aboard non-Subchapter H regulated towing vessels that push, pull or haul alongside tank vessels (towing vessels less than or equal to eight meters in registered length and some larger towing vessels that meet the exemptions listed in 33 CFR 104.105). The requirements of 46 U.S.C. 70105(b)(2)(C) and (D) will be further addressed in a future notice and comment rulemaking.

(d). Location of the Current 46 CFR 10.113 in the Proposed Rule

One commenter is confused over where the current 46 CFR 10.113 will be published in the new regulation.

Section 10.113 is part of the TWIC regulation, and will publish at that cite. It did not exist prior to this final rule, and is a new addition to part 10 along with a similar addition to part 12 at § 12.02–11. When the Coast Guard's ''Consolidation of Merchant Mariner Qualification Credentials'' rulemaking is finalized, it will be removed due to redundancy.

(e). Lack of Contingency Plan in Case of Disasters

One commenter demanded that there be a contingency plan created for those times when a natural disaster or emergency arise. When this happens, there may be a need to hire new maritime workers in a very short period of time to avoid disruption to the shipping industry and what it provides to the community.

We appreciate the concern shown by the commenter, but are not prepared, at this time, to write such provisions into the regulation. We do note, however, that 33 subchapter H includes procedures for obtaining approval for both waivers and equivalent security measures (*see* §§ 101.130, 104.130, 105.130, 106.125). In the absence of any specific contingency plan provisions, we believe that the waiver and equivalent provisions may be used to hire new personnel and allow them to work in a short time span. Additionally, Coast Guard is able to respond quickly in these situations and suspend any provisions that might disrupt the shipping industry in the wake of a natural disaster.

(f). Duplication of Applications and Background Checks for Merchant Mariners

One commenter supports the MTSA and the need for transportation workers to have an identification credential. This commenter also said these requirements should not be applied to American merchant mariners because of the extensive application process that merchant mariners currently undergo to obtain a MMD. American merchant mariners should be exempt from obtaining a TWIC if they possess a valid MMD and, in the future, a valid MMC. The MMD or MMC should serve as a federal identification credential.

We sympathize with the commenter, however 46 U.S.C 70105(b)(2)(B) clearly requires that U.S. mariners issued an MMD (as well as any other Coast Guard-

issued credential) obtain a TWIC. We recognized the duplication of effort that this might impose upon mariners, and as a result the Coast Guard has proposed consolidating its various credentials, and is working with TSA to ensure that as much information as possible will be shared between the two agencies, allowing mariners to apply for all of their required credentials after one visit to a TWIC enrollment center. Additionally, the Coast Guard will not be duplicating the security threat assessment; rather we will accept the TWIC as proof that the individual has been vetted for identification and security purposes. The Coast Guard inquiry will be limited to determining questions of safety and suitability. For more information on this effort, please see the Coast Guard's SNPRM entitled ''Consolidation of Merchant Mariner Qualification Credentials'' published elsewhere in today's **Federal Register**.

(g). Comments on Merchant Mariners

One commenter stated the large uncredentialed portion of the workforce (*e.g.*, towing vessels) needs to be identified and stabilized with immediate, adequate, and recorded safety and vocational training.

We agree with the concept that all mariners, both credentialed and non-credentialed, benefit from safety and vocational training. Although this comment is outside the scope of the TWIC regulations, which focus on identification and security, we note that existing regulations found in Title 46 of the CFR are in place to address these important issues.

One commenter expressed the view that Congress should reorganize the government to remove the superintendence of the U.S. Merchant Marine from the Coast Guard and return it to the U.S. Department of Transportation as a new agency.

Congressional reorganization of the U.S. Government is outside the scope of this regulation.

Another commenter would like to know why the TWIC card cannot be ''smart'' enough to be used as the qualification and identification credential.

We sympathize with this comment, and examined the possibility of combining the qualifications onto the TWIC. Unfortunately, it is not feasible at this time to have all of the qualifications listed on the face of the TWIC. STCW requires foreign port state control officers to be able to read a mariner's qualification credentials, and not all countries have the ability to read smart cards. It is impractical, and for some may be impossible, to print all of the information that will appear on an MMC on the face of the TWIC. We will, however, continue to explore options to allow for further consolidation between the two programs.

(h). Union Involvement

One commenter supported the program but urged that the rights of workers be preserved. The commenter was concerned that the program would restrict the civil rights of an employee to engage in collective and union activities and stated that wording should be incorporated into the rule to afford these liberties to all workers.

Nothing in either the NPRM or this final rule should be construed as having an effect on an employee's rights to collectively form or join a union. It is unnecessary to add anything to the regulation stating this explicitly.

(i). Written Request of Releasable Material Upon Initial Determination of Disqualification

The NPRM states that if an applicant wishes to receive copies of the releasable material upon which the Initial Determination was based, he must serve TSA with a written request within 60 days after the date of service of the Initial Determination. One commenter wanted TSA to automatically provide this information to the employee at the time of the determination for several reasons: (1) Employees may be denied employment during this process and writing a request and processing that request will delay possible employment; (2) requiring employees to request this information unduly burdens them (paperwork burden issue); (3) many employees will not have legal counsel and may not realize that they must make a special request for the information; and (4) by law, all appellants would be entitled to review the releasable material, and furthermore, this information is directly relevant to their appeal.

TSA provides applicants who receive an Initial Determination of Threat Assessment with the reason they do not meet the security threat assessment standards in the initial determination itself. The package that is mailed to the applicant includes the reason for the initial determination and information on how the applicant can appeal the determination. Therefore, in most cases the applicant will not need to request additional releasable information from TSA. TSA has prepared the information explaining the appeal and waiver process with applicants who are not represented by counsel in mind. The documents clearly and simply state the steps an applicant must take if an appeal or waiver is warranted.

(j). Interpretation of TWIC Requirements

One commenter urged interpretations to be centralized at Coast Guard Headquarters and disseminated to Coast Guard field offices. The commenter argued that COTPs should not be able to make individual interpretations and determinations of the rules, and added that this problem arose during MTSA implementation and led to inconsistent and inaccurate interpretations.

As stated elsewhere in this final rule, the Coast Guard intends to implement a robust guidance document to its field offices, in order to avoid inconsistent application of the regulatory requirements.

(k). Reporting of Incidents That May Result in a Transportation Security Incident

33 CFR 101.305(a) states that activities that may result in a transportation security incident are required to be reported by the owner/operator to the National Response Center (NRC). One commenter wanted this language to be amended to require reports to NRC for incidents that may ''reasonably'' be expected to result in a TSI. The commenter wants some clarification here to alleviate unnecessary and nonproductive reporting requirements.

We disagree with the suggested amendment. The NPRM did not include a proposed revision to § 101.305(a), and no change has been included in the final rule. Experience over the past three years indicates that the language of this section is not leading to any ''unnecessary and nonproductive'' reports to the NRC.

(l). Suggested Corrections To 33 CFR 101.515

One commenter requested three corrections/clarifications to § 101.515. First, to conform the personal identification requirements in § 101.515(a) with those in § 125.09, as set forth in the Coast Guard Notice, ''Maritime Identification Credentials'' that was published on April 28, 2006 (71 FR 25066), to be consistent as to what identification is required to access a part 105 facility. Second, in § 101.515(b), the reference to § (b)(4) should be to (a)(4). Third, clarify in § 101.515(c) that the facility has the right to escort law enforcement personnel for safety reasons and that such access does not imply unescorted access.

We have looked at the three suggestions, but have determined that

none of them are appropriate for action at this time. The second suggestion is not necessary, as the correct cross-reference is already listed. The first suggestion is not appropriate as the referenced Notice was intended as an interim security measure until TWIC could be implemented. We expect that, with implementation of this final rule, the Coast Guard will be able to announce that it will no longer be enforcing the provisions of 33 CFR part 125, as described in the referenced Notice. Finally, the third suggestion is not appropriate, as there may be times when requiring an escort would delay law enforcement officials, which is explicitly not allowed in § 101.515.

(m). Accredited Providers

One commenter wants DHS to explain the qualifying process a contractor must pass in order to be accredited. Since this was not in the NPRM, the commenter would like the opportunity to comment on this information once it is published.

The enrollment provider must adhere to all applicable laws, such as the Privacy Act of 1974 (5 U.S.C. 552a) and the Federal Information Security Management Act (44 U.S.C. 3541 et seq., Title III of the E-Government Act of 2002, Pub. L. 107–347) to protect the personal information that is collected and stored in the TSA System. In addition, all TWIC contractor employees who will have access to DHS sensitive information must have favorably adjudicated background investigations commensurate with the sensitivity level of the position held. The contractor must also maintain an IT Security Program where DHS data is stored or processed on contractor-owned information systems.

(n). Preamble Items Not Inserted Into the Rule

Three commenters complained that there were many requirements/issues mentioned in the preamble that were not incorporated in the rule. However, no specific examples were given. In light of this fact, we are unable to respond to this comment.

(o). Additional Uses of the TWIC

Two commenters would like to know if the TWIC card can be used for other commercial purposes not related to security. Specifically, one commenter would like to know if the TWIC card could be used as a payroll spreadsheet.

TWIC is designed to be used a tool for securing access control; however it is possible that it might be used for other purposes as well. The rule does not prevent alternate uses of the credential, as long as they do not interfere with the applications and information related to the standards in this rule.

(p). Accepted Cargo in Light of TWIC

One commenter assessed their business practices as a result of the implementation of TWIC and decided they would no longer move CDCs. They also said they would be forced to abandon their VSPs. The commenter is worried that other companies may do the same and not move these types of commodities. This would greatly hinder our economy and is not the intended effect of TWIC.

TSA and the Coast Guard have removed the card reader requirements from this final rule to reduce the potential burden on small businesses until such time as we can review additional technology and complete additional evaluation of the costs and benefits of reader requirements. Further details of the economic impacts of this final rule, including the costs imposed and the benefits gained, are identified in the accompanying Final Assessment.

(q). Interim Rules vs. Final Rules

One commenter wants the Coast Guard to address whether or not this rule will be published as a final rule as it incorporates, modifies, or updates regulations from the past that have never been published as a final rule.

This comment relates to interim final rules that the Coast Guard previously issued affecting STCW, licensing, and MMD regulations. The TWIC and MMC projects are not intended to serve as the final rules for those projects. At the completion of both TWIC and MMC, the Coast Guard intends to publish additional final rules addressing the comments received on the aforementioned interim rules, and make any necessary changes.

(r). NVIC

One commenter extended an offer to work with the Coast Guard in the development of an NVIC.

We appreciate the offer. We anticipate issuing a NVIC very soon. We also anticipate contacting many of our industry partners and engaging in as much industry consultation as possible prior to issuing a second NPRM proposing reader requirements.

C. TSA Provisions

1. Technology Concerns

TSA received a substantial number of comments on technology issues, almost all of which expressed concern about the feasibility and appropriateness of the proposal for reading the TWIC cards and verifying information. Commenters asserted that the TSA Prototype did not test many parts of the proposed system, including the readers and communications with a central database. Some raised questions about a central database. They questioned whether the systems will be compatible with existing systems and stated that if not, the costs of replacement will be high. Commenters stated that TSA must test the proposed system before requiring its use to ensure that it will work in the marine environment and that backup systems will function as well. They assert that TSA does not appear to have addressed issues related to system failures and power outages. In terms of interconnectivity, they stated that the system has to be shown capable of processing 700,000 TWIC instantaneously. Commenters also noted that the system does not appear to have been tested with passenger vessels.

As stated in the previous discussion on Coast Guard's provisions, the final rule will not require the owner/operator implementation of access control infrastructure, including readers. A notice of proposed rulemaking will follow this final rule that will address the use of access control readers for the TWIC program. Also, we must note that the TWIC program will not require continual interface with a 'central database' as implied in the comments.

The implementation of the TWIC program is different from Prototype in that TSA will not be involved with the port facility infrastructures and other ''systems'' referenced in these comments. Prototype created a testing environment for the credential that included Physical Access Control System (PACS) readers. The testing environment for Prototype included various environments and transportation modes, including marine locations.

Commenters also questioned TSA's assumption that the cards have a 5-year life cycle; the South Carolina State Port Authority said its experience indicated that cards do not last more than a year, which if true, would increase costs.

TSA believes the 5-year longevity of the TWIC is reasonable. There is very little data to permit a comparison of the credential referenced by the South Carolina State Port Authority to the durability of the TWIC. TSA will monitor card failures as the program is implemented and make changes to the credentialing system as needed.

Many commenters questioned the appropriateness of the FIPS 201–1 standard referenced in the NPRM and contact technology. They noted that it was developed for granting access to federal facilities and computer systems, not for granting access to ports and

marine facilities. They stated that it is slower, prone to errors, less reliable, and more susceptible to sabotage than contactless readers and cards. They noted that it has not been implemented at federal facilities yet. One commenter noted that smart cards can be copied.

DHS agrees that there are a number of challenges including biometric authentication, privacy controls, and security features. Therefore, we have established the NMSAC working group to recommend a contactless biometric specification for the TWIC program. In addition, when developing the card reader requirements, we will consider all of these concerns and implement a system that effectively serves a commercial environment.

A number of commenters noted that communications between vessels and a central database were uncertain and that some vessels do not have computers. They also noted that for some port facilities, locating the reader to handle arriving vessels can be problematic. Vessel operators stated that it is not feasible to install readers on many vessels.

Neither the NPRM nor this final rule discusses communications with a ''central database.'' The final rule does not require owner/operator implementation of access control infrastructure, including readers. A subsequent notice of proposed rulemaking will follow that will address the use of access control readers for the TWIC program.

Commenters questioned whether the reader technology required is ''intrinsically safe,'' as is required for facilities handling some hazmat.

All of the reader requirements have been removed from this final rule, therefore we do not need to address this comment at this time. We will, however, keep it in mind for our subsequent rulemaking on reader requirements, and the Coast Guard and TSA will work to ensure that new equipment will satisfy the applicable safety requirements. Furthermore, there should be no material impact on logistics or productivity based on the change from the NPRM. Vessels, facilities, and OCS facilities subject to this final rule already check individuals' identification credentials. This rule, therefore, should not introduce new requirements that would impact logistics or productivity.

2. Enrollment Issues

(a). Documents To Verify Identity

Commenters have asked what information an applicant must provide in order to verify identity when applying for a TWIC. Some commenters recommended that TSA adopt the documents listed as acceptable for identification purposes on U.S. Citizenship and Immigration Services (USCIS) Form I–9 ''Employment Eligibility Verification'' as acceptable documents to verify identity for TWIC purposes. Other commenters asserted that the documents listed on the current Form I–9 are subject to fraud.

TSA notes that the Form I–9 and its associated requirements are to verify that an individual is authorized under applicable immigration laws to work in the United States. The types of documents acceptable for a person to demonstrate his or her authorization to work may not in all instances be acceptable for TSA to verify identity for purposes of granting a credential that will allow the person access to a secure facility. If TSA believes that there is a significant risk that a type of document offered to verify a person's identity may be susceptible to fraud, we will not include that type of document in our list of identity verification documents for TWIC. As discussed above, the list of documents for identity verification for TWIC will be posted on the TWIC Web site and will initially include the documents accepted by TSA for persons applying for HMEs. DHS and other agencies within the federal government, however, continue to review identity documents to ascertain that those which are most susceptible to forgery, fraud, or duplication are not used, among other things, to obtain government security credentials. TSA may change the list of acceptable documents in the future consistent with that review.

In addition, the REAL ID Act of 2005, Pub. L. 109–13, 119 Stat. 312 (May 11, 2005), requires implementation of minimum document requirements and issuance standards for State-issued driver's licenses intended for use for official federal purposes. The REAL ID Act requires that, effective May 11, 2008, a State that participates in REAL ID will adopt certain minimum standards to: (1) Authenticate documents produced by applicants to prove identity and lawful status in the U.S., (2) ensure the integrity of the information that appears on driver's licenses and identification cards, and (3) prevent tampering, counterfeiting or duplication of such cards for a fraudulent purpose. Under the REAL ID Act, DHS is authorized to promulgate regulations to determine whether States driver's license standards are in compliance with the REAL ID Act.

The standards for documents accepted for identity verification for TWIC purposes would necessarily be affected by any regulations issued to implement the REAL ID requirements and will likely result in a change in the accepted document list for TWIC once the REAL ID regulations are implemented.

For all mariners, the enrollment section now provides that merchant mariners must bring the documents that the Coast Guard requires in 46 CFR chapter I, subchapter B to verify citizenship and alien status. The proof of citizenship requirements are currently contained in 46 CFR 10.201 for licenses and CORs, and 12.02.13 for MMDs. The Coast Guard has proposed changing these citizenship requirements as discussed in the MMC SNPRM published elsewhere in today's **Federal Register**. We are requiring that mariners bring these documents to the TWIC enrollment center because they must be scanned into the enrollment record so that the Coast Guard has them available to review when reviewing the merchant mariner's record to renew or obtain an MMC.

(b). Where Enrollment Should Begin

A few commenters opposed implementation at the largest ports until the TWIC program has been tested in other areas first, to minimize adverse impacts on the national economy.

To mitigate security threats at the ports, TSA and the Coast Guard have developed a phased deployment for the TWIC program over an 18-month period. The deployment of TWIC enrollment centers will start with a small number of ports, and ports will be added over time across the TWIC population centers. The scheduling of the deployment by TSA and the Coast Guard is based on the Coast Guard's list of ports, ranked by size and criticality. The deployment schedule will be closely coordinated with the COTP in the various regions.

(c). Other Timing Issues

Some commenters thought that the schedule for implementing the program within 18 months is unrealistic. Others urged TSA to extend the implementation period to allow testing of biometric readers or to allow the Coast Guard to redesign its MMC to incorporate TWIC security features.

We believe the 18-month timetable for conducting the initial enrollment is realistic. If unforeseen events delay completion of the initial enrollment, we will adjust the schedule accordingly and notify all affected workers and owners/operators.

One commenter believed that the 5-year TWIC renewals should be staggered. Another commenter suggested that the TWIC should be

considered good, even if expired, based on receipt by TSA of a valid application or renewal. Others supported the 180-day window for renewals for mariners, but asked whether the same window would apply to non-mariners employed on covered vessels. The phased deployment of enrollment centers will result in staggered TWIC enrollment. The deployment approach will spread out the enrollment population to different geographic locations as the deployment progresses across the maritime sector. All affected workers should plan for renewals based on their respective schedules and locations. The NPRM specifically mentioned a 6-month period for mariners because they must complete the check for the mariner's license, which is time-consuming, following the threat assessment for TWIC.

Some officials from the State of Florida suggested that the Florida identification cards currently in use could be replaced with the TWICs as the Florida cards expire. State-issued identification cards will not be considered comparable to or interchangeable with TWIC, and therefore, the commenter's suggestion cannot be accepted.

Others asked how the scheduling system would interact with ports and port enrollment personnel, and urged TSA to give consideration to current workers to minimize disruption to commerce.

TSA and the Coast Guard will work closely with the COTPs and industry to ensure that all affected employers and workers know when enrollment will begin at the nearest location. Much of the enrollment information for TWIC, including some scheduling items, will be available on-line. We will publish Notices in the **Federal Register** as the enrollment schedule unfolds, so that all affected workers, including individuals who do not work regularly on a vessel or maritime facility, can determine when he or she should enroll and where to complete enrollment. All applicants are encouraged to pre-enroll on-line and schedule an appointment at the enrollment center to complete enrollment. In addition, owners/operators must give 60 days notice to employees to provide employees with adequate notice to schedule TWIC enrollment during the initial enrollment roll out.

(d). Additional Enrollment Centers

Many commenters believed there should be more enrollment centers at convenient locations to minimize travel and missed work. Some commenters were concerned that the number of centers in highly industrialized areas would not be adequate, and some named specific locations, such as Oakland, California and Paducah, Kentucky that need centers. Others thought there was a need for centers at ports in Alaska, such as Juneau; at out-of-the-way places such as Kodiak and Dutch Harbor, Alaska and the U.S. Territory of Guam; and at locations outside the United States for mariners on job assignments overseas. A commenter asked about renewals for individuals who are residing overseas and do not have ready access to an enrollment center.

We agree and, where applicable, we may use mobile enrollment centers for the phased enrollment approach. Based on commenters' input, Juneau and Guam have been added as ports that will be covered. The Port of Oakland is on the list. The area of Paducah is a 3–5 hour drive from centers located in St. Louis, Chattanooga, Nashville, Louisville and Memphis. These areas, as well as others mentioned in Alaska, will be reviewed during the implementation. The number and location of enrollment centers will balance the need for convenience with the cost of additional enrollment centers to avoid increasing the financial burden on applicants.

A few commenters noted that centers should be readily accessible to trucks and that centers should be kept open around-the-clock if that is where workers would go to reset their PIN. One commenter recommended that the procedures for changing a PIN be clarified. Several commenters suggested making use of existing facilities, such as offices of CBP, motor vehicle offices, law enforcement offices, post offices, Coast Guard RECs, sector command centers, and enrollment centers used for the Florida identification card. Commenters also encouraged the use of mobile centers that could visit ports and major facilities and could return more than once so that applicants could use the mobile center again.

We agree and, as stated above, will use mobile enrollment centers where appropriate for the phased-in enrollment approach. TSA also agrees that alternate hours of operation at enrollment centers will reduce the burden placed on TWIC users. Enrollment center hours of operation will balance the need for convenience with the cost of additional personnel for extended enrollment center hours, to avoid increasing the amount of the fee for the applicants. The contractor selected for enrollment may use existing facilities as it deems appropriate.

(e). Picking Up Credentials at an Alternate Center

Several commenters supported the idea of allowing applicants to pick up their credential at an alternate location. Some noted that mariners aboard a vessel may not be able to return readily to the same enrollment center.

TSA appreciates the commenter's suggestion, but under the current implementation plan, the system cannot be altered to accommodate retrieving credentials from an alternate location. TSA is working to include this kind of option in the future. For now, aside from the software design issue, TSA believes that without further analysis or testing, this process may unreasonably complicate the accountability and shipment of the cards from the production facility. If an applicant cannot retrieve the credential shortly after being notified that it is ready, the enrollment center will hold the card until the applicant returns to pick up the credential.

(f). Other Ways To Ease the Process

A few commenters believed that facilities and employers should be allowed to capture all applicant information, including the biometrics, and activate the credentials. Some suggested that the CSO could activate TWICs on behalf of the enrollment centers. One commenter suggested using a passport, which includes a specific check for identity by the issuing office, in place of the TWIC. Two commenters asked how enrollment will be accomplished for mariners abroad and whether U.S. consulates could play a role.

Based on industry comments received during Prototype, we do not require individual companies to act as sponsors and assist in the enrollment process. In addition, given the economies of scale, the cost of enrollment is lower by using one contractor. It is also important to maintain consistency in procedures across the country and ensure that only Trusted Agents who are adequately trained conduct enrollment and card activation.

We do not agree that a passport is a good alternative to TWIC. TWIC is a biometric credential with multiple security, identification, and authentication features; a passport does not contain many of these features, such as a biometric, which are required by MTSA.

The Coast Guard and TSA are examining methods to ensure that mariners stationed overseas will have adequate opportunities to enroll for TWIC. This process may involve

sending TWIC enrollment personnel overseas for a short time.

(g). Other Enrollment Center Issues

Commenters raised a number of miscellaneous suggestions and questions regarding enrollment. Commenters asked how TSA would address post-enrollment maintenance of the enrollment centers.

After the initial 18-month deployment of enrollment centers, TSA will determine the needs for post-enrollment maintenance of enrollment centers based on population, turnover, and other factors related to enrollment.

Commenters suggested that the criminal history portion of the threat assessment should be conducted in the applicant's State of residence because criminal codes vary from State to State.

TSA will leverage existing tools and personnel to conduct security threat assessments. All of the CHRCs will go through the FBI's Criminal Justice Information Service (CJIS), which is the national repository for criminal records. It is true that criminal codes may vary from State to State, but the adjudication staff and attorneys with criminal law expertise who support the adjudication process are experienced in examining State conviction records to determine if a disqualifying offense in § 1572.103 of the rule has occurred.

Commenters asked if there would be accommodations for individuals who cannot produce 10 fingerprints due to injury. For purposes of the CHRC, TSA will consult with the FBI and utilize the procedure it has in place for individuals who cannot produce 10 fingerprints.

Commenters asked if making an appointment for completing enrollment provides a defined time slot for service.

As planned, the appointment process will allow the applicants to schedule a time for enrollment in 15- to 30-minute increments at a specific enrollment center. The center will also accommodate walk-in enrollees, but will provide preference to those with appointments.

Commenters asked what method of payment would be acceptable for the TWIC fee. TSA will accept payment by credit card, cashier's check, or money order.

Commenters asked if enrollment centers will be located at ports, and if port personnel will be used to enroll applicants. Also, commenters asked if the enrollment staff will be trained.

TWIC enrollment centers will be staffed by TSA contractor personnel—Trusted Agents, not port personnel. All Trusted Agents will undergo a TSA security threat assessment and complete specialized training before conducting enrollment. TSA and the Coast Guard are currently considering that the enrollment centers will be within a five-mile radius of the center of the port population, where possible.

(h). Use of E-Mail for Notifications and Correspondence

A commenter asked if e-mail could be used in place of paper notifications and correspondence, and supported it as a means for cost savings. A commenter suggested allowing at least one alternate method for transmitting notifications and correspondence to applicants.

TWIC enrollees will be notified via e-mail or voice mail that their card is ready. TWIC applicants are asked to express a preference for one of these methods, and should select the one they are most likely to receive when sent. However, the notifications that TSA must provide following completion of the security threat assessment must be through the U.S. mail at this time. The infrastructure TSA currently uses for HME applicants involves the electronic production of letters that have been created to fit all potential threat assessment outcomes and transmission by U.S. mail. For the TWIC initial enrollment and the HME process, TSA cannot change this existing system, but will expand the system to accommodate e-mail notifications in the future.

(i). Lost, Damaged, or Stolen TWICs

Several commenters made reference to the need to report a lost or stolen TWIC immediately.

We agree with this comment. Lost, damaged, or stolen TWICs must be reported to TSA in accordance with § 1572.19(f). They should be reported to the TWIC Call Center, which will have a readily available number, as soon as the card is determined to be missing or damaged. After the applicant submits payment for the replacement TWIC card, the TWIC system will then automatically send a signal to the card production facility to trigger production of a replacement TWIC. TSA will add the lost/damaged/stolen credential to the list of revoked cards for which access to secure areas cannot be granted, to guard against the credential being used by someone other than the rightful holder. Additionally, reporting the card is a necessary step if the individual continues to require unescorted access.

One commenter stated that if an employee can demonstrate proof that the TWIC was stolen, the fee for a replacement TWIC should be waived.

We do not agree with the comment. It would be very difficult to establish with certainty that a TWIC was stolen before a replacement card is ordered, and developing standards for determining this to apply consistently at all enrollment centers would be equally difficult. In addition, for security reasons applicants must handle their credentials carefully so that they do not fall into the hands of others.

Several commenters expressed concern about the burden of requiring an applicant to appear at an enrollment center to report a lost or stolen card (as required in the Prototype). According to these commenters, the inconvenience of traveling to an enrollment center is exacerbated for mariners serving on vessels engaged in international voyages or on domestic voyages where the lack of proximity to an enrollment center would make it very difficult to mandate a personal appearance in a timely manner, especially considering the 24 by 7 watch schedules on commercial vessels. Several commenters requested that individuals be able to order a replacement TWIC via the Internet and then validate his or her biometrics and activate their TWIC during a single trip to an enrollment center.

We agree with these comments, and applicants should report lost, damaged or stolen credentials through the TWIC Call Center. TWIC holders will have to visit an enrollment center once to pick up and activate their replacement TWIC.

(j). Employer Responsibility To Notify Employees

A commenter remarked that such a requirement should not be for individual notice, but should be fulfilled by a posting. The commenter expressed concern that if an individual is not notified and subsequently is determined to pose a threat of terrorism or engaged in terrorist activity, the owner/operator might be liable for any damages that result.

We recognize that an owner/operator may have a variety of means at his or her disposal to communicate with employees. The requirement does not specify that the notice be given to each employee individually, but whatever mean is chosen (and there may be more than one) it should be aimed at reaching as many employees as possible.

One commenter requested confirmation that TSA had stored the fingerprints and biographical information of HME driver-applicants.

TSA stores the fingerprints and biographic information of HME applicants who are licensed in States that use TSA's agent to conduct enrollment.

3. Appeal and Waiver Issues

(a). Independent Review by Neutral Party

Several commenters urged TSA to modify the appeal and waiver processes to include an independent review by a neutral party, such as an ALJ. TSA issues an Initial Determination of Threat Assessment if the results of the threat assessment reveal a disqualifying standard. In the proposed rule, TSA stated that if legislation were enacted after publication of the proposed rule that requires TSA to adopt a program in which ALJs may be used to review cases in which TSA has denied a waiver request, TSA would amend the final rule to address such statutory mandates. 71 FR at 29421. On July 11, 2006, the Coast Guard and Maritime Transportation Act of 2006 was signed into law. H.R. 889, sec. 309, amending 46 U.S.C. 70105(c). The Act mandates the creation of a review process before an ALJ for individuals denied a waiver under the TWIC program. As a result, we have added procedures for the review by an ALJ for requests for waivers that are denied by TSA. These procedures are discussed in detail above in ''TSA Changes to the Proposed Rule.''

(b). Deadlines for Appeal and Waiver Processing

Several commenters argued that it would be difficult for individuals who travel for extended periods of time to comply with the 60-day deadline for appealing an adverse determination or requesting a waiver. Some of these commenters also noted that TSA's definition of ''date of service'' provides for constructive notice but does not ensure actual notice.

While the proposed rule allowed applicants to apply for an extension of the deadline, the request for extension had to be in writing and received by TSA within a reasonable time before the due date to be extended. TSA understands that if individuals have difficulty complying with the 60-day deadline for appealing an adverse decision or requesting a waiver, individuals may have equal difficulty requesting an extension within the timeframe allowed. For these reasons, TSA is amending its appeal and waiver procedures to allow requests for an extension even after the deadline for response has passed. Individuals will now be allowed to request an extension of the deadline after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline. We believe this amendment makes the appeal and waiver processes more reasonable for the group of workers affected.

(c). Facility Owner's Role in TWIC Appeal Process

One commenter said that the adjudication process for information developed during the security threat assessment is flawed and undermines the facility owner's responsibility because it does not involve the owner/operator of a facility. The commenter said that a facility owner might have information that could allow the appeal to be decided quickly. The commenter said that the proposed appeal process conflicts with the facility owner's ultimate responsibility for the security of his facilities and that it could create significant liability issues for facility owners. The commenter stated that the ultimate responsibility for determining an individual's eligibility for unescorted access to critical facilities must remain with the owner of that facility.

We disagree. The statutory language of 46 U.S.C. 70105 specifically prohibits sharing of information with an applicant's employer: ''Information obtained by the Attorney General or the Secretary under [sec. 105 of the MTSA] may not be made available to the public, including the individual's employer.'' It further provides that ''An individual's employer may only be informed of whether or not the individual has been issued the card under [sec. 70105 of the MTSA].'' An applicant may offer any information during an appeal or waiver process that he or she feels is relevant to the appeal or waiver process, including information from the employer on his or her behalf that the applicant feels will assist the adjudicators in making a decision.

The TWIC process does not create a liability issue for facility or vessel owner/operators. The ultimate responsibility for decisions as to who should be allowed entry, and under what conditions, remains with the owner/operator, so long as only TWIC holders are given unescorted access to secure areas. The TWIC system enhances his or her ability to make that decision by providing a highly reliable source of information regarding the known risks presented by an individual requiring access. The owner/operator can therefore make informed, confident choices in deciding whether or not to grant access and under what conditions. Furthermore, since the owner/operator is removed from the adjudication process, he or she is further protected from increased liability, since all challenges to the adjudication process will necessarily be directed at the federal government, not the owner/operator.

4. TSA Inspection

In proposed § 1572.41, TSA proposed to require owners/operators to permit TSA personnel to enter the secure areas of maritime facilities to evaluate, inspect, and test for compliance with the standards in part 1572. Many commenters recommended that the Coast Guard serve as the primary inspection authority. Several commenters expressed uncertainty regarding whether or the degree to which TSA's envisioned responsibility for auditing TWIC readers implies a role for TSA in compliance checking. Some commenters suggested that the Coast Guard be responsible for all vessel and facility inspections, particularly those that entail boarding vessels. One commenter recommended an MOA between the Coast Guard and TSA and one suggested that TSA access TWIC readers under the Coast Guard oversight. Another commenter recommended that TSA delete 49 CFR 1572.41, not implement a TSA inspection program, and revise 33 CFR 101.400 and 33 CFR 101.410 to add TWIC compliance to existing Coast Guard vessel and facility security inspection programs.

In accordance with our statutes, TSA and the Coast Guard have joint responsibility for development and oversight of the TWIC program. In addition, both agencies have statutory authority to inspect for compliance with their regulations and to conduct security assessments. The intent of adding specific language to the regulation regarding TSA's inspection authority is not to add additional burdens to the maritime industry but to clarify the existing authority and inform the public of their statutory obligations. To address the concerns expressed by the maritime industry and promote consistency, Coast Guard and TSA field guidance will be developed and include the need for coordination of TSA inspections or tests with the local Coast Guard COTP or his/her representative.

The inspection rule language has been moved to 49 CFR 1570.11, where it fits organizationally among the other general requirements. This section is similar to those in other modes of transportation and is necessary for TSA to exercise its oversight and enforcement responsibilities over trusted agents, the enrollment process, and the performance of the credential in a variety of circumstances.

5. Security Threat Assessment

(a). Comparability of Other Background Checks

We received many comments on proposed § 1572.5(d), in which TSA described a process to determine if security threat assessments or background checks completed by other governmental agencies can be deemed comparable to TSA's threat assessment for TWIC and HME, to minimize redundant assessments. Generally, commenters supported the concept of recognizing the background checks of other government agencies as comparable. Many argued that maritime workers may have a government ''Secret'' or ''Top Secret'' clearance and should not be required to undergo a TWIC threat assessment. Commenters from marine services companies, shipping and cruise lines, towing companies, and maritime organizations stated that background checks performed by employers should alleviate, in whole or part, security concerns and make TWIC unnecessary. Some said that company ID badge programs adequately address the security issues. Some commenters said the name checks currently being conducted on port workers created adequate safeguards. Two commenters said that they should have an opportunity to demonstrate to TSA that their credential program qualified as an alternate to TWIC and could be designated as ''TWIC equivalent.'' One commenter noted that TWIC would need to cover persons who are not normal seaport employees, such as Federal postal service employees. One commenter pointed out that background checks for unescorted access to the Secure Identification Display Areas of an airport are equivalent to or more stringent than the background checks under the proposed rule. One commenter noted that certain utility workers are already subject to more stringent security measures such as Nuclear Regulatory Commission requirements. One commenter requested that the final rule recognize the equivalency of the DOD National Industrial Security Program (DOD NIST) and the U.S. Office of Personnel Management's Trustworthy Determination review and clearance programs. Several commenters supported the fact that the proposed rules will accept a background check done for a hazardous materials endorsement or under CBP's FAST program.

TSA is pleased that this section is generally favored by the industry and we are not making any changes to the language proposed in the NPRM. TSA looks forward to working with other governmental agencies, many of which were cited in the comments, to issue comparability determinations where appropriate and eliminate duplicative checks. When a comparability decision is made, TSA will announce the decision through a Notice in the **Federal Register**. Fees will be reduced in the same manner described in this rulemaking for holders of HMEs.

We do not believe it would be advisable to offer comparability determinations to private companies for the checks they perform on the workforce. A check conducted by a private employer would not include the in-depth review of information related to terrorist activity and organizations to which TSA has access. These checks are critical to making the security determination that MTSA requires.

(b). Adjudication Time

The proposed rule preamble states that facility and vessel owners/operators must notify workers of their responsibility to enroll and that generally, owners/operators should give individuals 60-days notice to begin the process. Many commenters objected to this timeframe, referring to it as a ''60-day waiting period.'' One commenter urged TSA to dedicate additional resources to ensure the system has the capacity to handle the processing load. Other commenters believed that completing the threat assessment in less than 30 days is optimistic.

Many commenters urged that the time needed to complete an applicant's adjudication should be shortened. Several pointed out that during TWIC Prototype testing, the goal was 96 hours from enrollment to receipt of the card, and commenters favored this time period. A few commenters asked why the period could not be shortened to 24 or 48 hours, and others suggested 5 days, which is the standard in Florida. Some asked why we could not adopt the check completed for purchasing a firearm. A commenter noted that the in legislative history of MTSA, members of Congress expected that DHS would be able to issue a TWIC within 72 hours of receipt of an application. Others, including local port authorities and associations, did not give a specific timeframe but thought the processing time could and should be reduced. One commenter asked TSA to provide expedited or prioritized application service for merchant mariners who are often absent for many months at a time. One commenter recommended that TSA should consider issuing a temporary credential for those individuals who are attempting to rectify a problem that surfaced in the adjudication process, which might stem from a case of mistaken identity or inaccurate court records.

First, it is important to state that the TWIC program does not have a mandatory ''waiting period.'' Rather, TSA must adjudicate the security threat assessment of each applicant following enrollment and each case necessarily entails processing time. During the initial enrollment roll out, owners/operators must give ample notice to workers so that the threat assessment can be completed before the workers are required to present a TWIC to gain access to secure areas. As a general rule, security threat assessments and issuance of a TWIC should take no longer than 30 days. In fact, in our experience completing the threat assessments for hazmat drivers, threat assessments are typically completed in less than 10 days and we will strive to keep the threat assessment time period to 10 days for most applicants. However, processing time increases for an applicant with a criminal history or other disqualifying information, and is further lengthened if the applicant initiates an appeal or waiver.

Criminal records are not standard and are often incomplete or out-of-date. When a rap sheet is revealed following submission of an applicant's fingerprints, an adjudicator must review it carefully and often must make additional inquiries in other public court data sources or telephonically to determine if a disqualifying offense has occurred, and if it occurred within the prescribed time period. In addition, often the adjudicator must contact another agency that may be engaged in an investigation of the applicant, to determine the nature of the investigation, if it involves security-related issues, and whether going forward with an Initial Determination of Threat Assessment would inappropriately signal to the applicant that an investigation is ongoing. This process can be very lengthy, and one over which TSA generally has no control.

The time period needed to complete security threat assessments during the TWIC prototype is not a good model from which to make comparisons. TSA was not able to complete a CHRC during Prototype, because there was not a regulation in place requiring a fingerprint-based check. Therefore, the time needed to complete the threat assessment was much shorter than is typical. However, the Prototype provided data on enrollment and card production processing times. We will

process applications as they are received. After applications are received and sent for security threat assessment, individual processing times will vary based on the complexity of the adjudication.

The check done when an individual wishes to purchase a firearm differs from this check in many respects. The firearms check was created before the terrorist attack on September 11, and has a different purpose. The government reviews different records for that check, which do not require fingerprints to search. No credential is issued and no biometric is used to verify identity, so the system needed to support the program is less complex. The volume of applicants is lower than in TSA's security threat assessment programs and there is a different funding mechanism for the firearms search.

In response to the many comments on adjudication time, TSA is amending the information required or requested for enrollment to help expedite the adjudication process. Most of the new information is voluntary; however, providing it should help TSA complete adjudications more quickly. All of the amendments apply to HME and TWIC applicants. First, applicants who are U.S. citizens born abroad may provide their passport number and Department of State Consular Report of Birth Abroad. These documents expedite the adjudication process for applicants who are U.S. citizens born abroad. In addition, applicants who have previously completed a TSA threat assessment should provide the date of completion and the program for which it was completed. Also, applicants are asked to provide information if they hold a Federal security clearance, and include the date the clearance was granted and the agency for which the clearance was performed.

We considered issuing a temporary credential to individuals while their threat assessment is underway, but determined it would create more problems than it would solve. First, the fee to each applicant would increase dramatically. Second, an entirely new software system would have to be developed to implement a temporary credential. For a simple system, the temporary card would probably not contain a biometric or photograph, and so the opportunities for misuse would be great.

The Coast Guard has had experience with issuing temporary credentials. In the late 1970s, the Coast Guard issued temporary MMDs, in the form of a letter, to allow an applicant to sail for six months during which time the applicant could decide if he or she wanted to remain a seafarer. No commitment of employment was required. This soon became an administrative burden with the applicant obtaining a temporary MMD, sailing for awhile, and then finding better employment ashore. In addition, the Coast Guard had many records of issuance with no closure because the applicant never returned to apply for a final MMD.

A general review of background checks and security threat assessments across government and in the private sector will show that the TSA processing time for a TWIC or HME is far below the average time to complete an assessment. Many threat assessments take six months or longer. In any event, as described above in the discussion of the Coast Guard's provisions, we have included a provision in the final rule to provide relief to the owner/operator who absolutely must provide a new direct hire with access to secure areas before the individual's TWIC has been issued.

(c). Disqualifying Criminal Offenses

We received a variety of comments concerning disqualifying criminal offenses. We changed this section in response to comments, and the changes are discussed in detail above in the ''TSA Changes from the Proposed Rule.'' We received some very specific comments that we will address here.

Several commenters including port authorities recommended that cargo theft be added to the list of disqualifying crimes. Depending on the circumstances of the conviction, TSA believes that, in most cases, cargo theft will be covered by § 1572.103(b)(2)(iii) dishonesty, misrepresentation, or fraud.

Some commenters suggested that improper transportation of hazardous materials could encompass neglecting to placard a vehicle or to replace a placard that fell off. Also, commenters are concerned that a transportation security incident could include an environmental spill caused by negligence. TSA does not agree. Improper transportation of a hazardous material under 49 U.S.C. 5124 requires that the violation be knowingly, willfully, or recklessly committed. To be disqualified under the rule, the applicant must have received a felony conviction for improper transportation of hazardous materials or a transportation security incident. A felony conviction for these crimes reflects evidence of serious criminal culpability for conduct directly related to proper transportation procedures and port security. Both of these offenses are waiver eligible, and TSA may evaluate the applicant's conduct, intent, and other circumstances of the conviction as part of the waiver process.

Other commenters suggested that ''improper transportation of a hazardous material'' and ''unlawful possession of an explosive or explosive device'' should not permanently disqualify someone from obtaining a TWIC. TSA disagrees. These offenses have always been permanent disqualifiers. Because of the dangerous nature of explosives, a felony offense involving hazardous or explosive materials is highly relevant to a person's qualifications to transport hazardous material or to have unescorted access to secure areas. As TSA stated in the NPRM, after reviewing all of the individual circumstances, TSA has granted waivers for prior nonviolent felony convictions for illegal possession of an explosive.

Commenters noted that States define crimes differently and that these inconsistent standards may lead to unequal standards for denying individuals employment. Where necessary, TSA evaluates an applicant's State conviction by comparison to the State crime to the elements of the applicable federal crime. TSA may review the individual circumstances of a conviction, including the elements of the crime as defined by a particular State, if the crime is identified as one for which the applicant may be eligible for a waiver and the applicant seeks a waiver from disqualification.

TSA also received several comments suggesting that the language was unclear explaining how prior convictions and incarceration count to disqualify an applicant. TSA has revised the language to clarify that the crimes listed are disqualifying if either of the following is true: (1) The applicant's date of conviction is within seven years of the date of application; or (2) the applicant was incarcerated for that crime and was released from incarceration within five years of the date of application.

Requests for ''grandfathering,'' that is, waiving all or certain disqualifying crimes for individuals who have been working on a MTSA-regulated facility or vessel prior to the implementation date for TWIC, were carefully considered and evaluated at length during the public comment period and drafting of the final rule. We have decided not to include a grandfathering provision in order to ensure that all individuals who are issued a TWIC have successfully completed a published and consistent threat assessment process. Part of the purpose in implementing TWIC is finding out who is in our ports; we do not think it is appropriate to allow unescorted access to an individual who may pose a terrorism risk merely

because he or she has worked in the maritime environment for a period of time without incident. Doing so presents an unacceptable security risk. However, in order to address the industry comments and concerns over losing a significant population of the work force due to an inability to apply for and receive a TWIC due to the disqualifying crimes requirement, the list has been modified, and the waiver appeal process has been enhanced to include independent third party evaluation.

Several commenters opposed § 1572.107 which grants TSA the ability to disqualify individuals for crimes that are not included on its list, as this would be too subjective or applied inconsistently. Others commented that § 1572.107(b) violates due process as it allows TSA to disqualify an individual merely ''suspected'' of posing a security threat.

TSA believes that this is a necessary provision, as it is impossible to list every crime that may be indicative of a threat to security. Further, § 1572.107 is not often used to disqualify persons for criminal convictions, and part 1515 requires a different level of review than a determination based on the list of disqualifying crimes.

Paragraph 1572.103(d) describes how an arrest with no indication of a conviction, plea, sentence or other information indicative of a final disposition must be handled. TSA is changing the time allowed for an applicant to provide correct records from 30 days to 60 days. The individual must provide TSA, within 60 days after the date TSA notifies the individual, with written proof that the arrest did not result in a conviction of a disqualifying criminal offense. If TSA does not receive such proof within 60 days, TSA will notify the applicant that the he or she is disqualified from holding an HME or a TWIC.

One commenter stated that preventing individuals who are wanted or under indictment for listed felonies from obtaining a TWIC is inappropriate since only those that have been ''convicted'' can be denied a security card.

An individual under want or warrant is a fugitive from justice and therefore is not a suitable candidate for a TWIC. In addition, the return of an indictment for a disqualifying crime reflects a preliminary finding that there is, at a minimum, reasonable cause to believe that the individual committed the disqualifying crime. Therefore, TSA has determined that persons who are the subject of a pending indictment for one of the crimes on the list should be disqualified from obtaining TWICs. If the indictment is subsequently dismissed or, after trial, results in a finding of not guilty, the applicant is no longer disqualified and may reapply for a TWIC.

A commenter asked TSA to reconsider the practice of considering a guilty plea a conviction for purposes of this section. TSA applies federal law to determine whether the disposition of a criminal case constitutes a ''conviction.'' In *Dickerson* v. *New Banner Institute, Inc.,* 460 U.S. 103 (1983), the United States Supreme Court held that the defendant had been convicted for the purpose of a federal gun control statute even though under state law, the defendant's sentence had been deferred. The fact that the defendant pled guilty to the state offense was sufficient to constitute a conviction for the purposes of federal law. This case supports a broad interpretation of the term ''convicted,'' for purpose of this final rule.

(d). Waivers

It is important to highlight here that applicants who are disqualified due to a criminal conviction should make every effort to apply for a waiver, assuming the crime is waiver-eligible. TSA has developed the waiver program to ensure that individuals who have a criminal history but no longer pose a threat are not denied an HME or a TWIC. The process is informal, designed for applicants who are not represented by counsel and are not conversant with legal terms and process. We accept hand-written waiver applications, so the applicant does not need to have a computer.

In determining whether to grant a waiver request, we are most interested in the circumstances surrounding the conviction, the applicant's history since the conviction, the length of time the applicant has been out of prison if sentenced to incarceration, and references from employers, probation officers, parole officers, clergy and others who know the applicant and can attest to his or her responsibility and good character. TSA grants the majority of waiver applications received.

6. Immigration Status

Commenters asked the TSA to extend TWIC eligibility to non-resident aliens who are lawfully admitted into the U.S. under visas that permit them to work. Another commenter noted that maritime owners/operators bring in specialists from around the world to complete specialized tasks on vessels, and these workers should be able to apply for and obtain a TWIC. One commenter suggested that applicants should have to show U.S. residence for three years to apply for a TWIC. Several commenters noted that multinational corporations involved in the maritime industry have foreign employees and foreign business partners at U.S. facilities, and these individuals should not have to be escorted through secured facilities or vessels.

The NPRM was drafted to permit non-resident aliens in the U.S. with authorization to work here to apply for and obtain a TWIC, so the first two commenters' concerns are not warranted. TSA and the Coast Guard considered the relatively common employment of foreign specialists in certain maritime job categories when developing the immigration standards. This final rule allows holders of certain categories of nonimmigrant visas, with work authorization, to apply for a TWIC.

For purposes of this discussion, it is helpful to explain that there are two categories of U.S. visas: immigrant and nonimmigrant. As provided in the immigration laws, an immigrant is a foreign national who has been approved for lawful permanent residence in the United States. Immigrants enjoy unrestricted eligibility for employment authorization. Nonimmigrants, on the other hand, are foreign nationals who have permanent residence outside the United States and who are admitted to the United States on a temporary basis. Thus, immigrant visas are issued to qualified persons who intend to live permanently in the United States. Nonimmigrant visas are issued to qualified persons with permanent residence outside the United States, but who are authorized to be in the United States on a temporary basis, usually for tourism, business, study, or short or long-term work. Certain categories of lawful nonimmigrant visas or status allow for restricted employment authorization during the validity period of the visa or status.

An alien holding one of the following visa categories is eligible to apply for a TWIC: (1) H–1B Special Occupations; (2) H–1B1 Free Trade Agreement; (3) E–1 Treaty Trader; (4) E–2 Treaty Investor; (5) E–3 Australian in Specialty Occupation; (6) L–1 Intra Company Executive Transfer; (7) O–1 Extraordinary Ability; or (8) TN North American Free Trade Agreement. In selecting these visa categories, we focused on the professionals and specialized workers who are frequently employed in the maritime industry to work on vessels or other equipment unique to the maritime industry. In addition, we understand that many Canadian and Mexican citizens conduct business at ports in the United States,

and barring them from obtaining a TWIC would create an undue burden on commerce. Also, we are adding foreign nationals who are attending the U. S. Merchant Marine Academy to the group of aliens who may apply for a TWIC, if they are in proper visa status. Finally, we are including applicants from the Marshall Islands, Micronesia, and Palau as eligible to apply for a TWIC. The United States has entered into treaties with these countries and shares close ties with each of them. Citizens of the Marshall Islands, Micronesia, and Palau may reside in the United States indefinitely and have unrestricted authorization to work here.

In order to minimize the likelihood that an applicant with a short-term visa retains a 5-year TWIC, we are requiring the employer of any individual holding an eligible nonimmigrant visa to retrieve the TWIC from the employee when the visa expires, the employer terminates the employment, or the employee otherwise ceases to work for the employer. In addition, we require the employee to surrender the TWIC to the employer. If the employer terminates the employee, or the employee ceases working for the employer, the employer must notify TSA within five business days and provide the TWIC to TSA if possible.

7. Mental Incapacity

One commenter believes that the NPRM inaccurately treats illnesses like drug addiction as indicators of mental incapacity if commitment to an institution results. Another commenter representing port employers stated that some port workers have very low IQs and consequently have been assigned legal guardians, but work successfully in port facilities.

TSA agrees that such applicants can be determined to be qualified to hold a TWIC or HME. As discussed above in the ''TSA Changes to the Proposed Rule,'' TSA has no interest in limiting the ability of mentally-challenged or ill workers to obtain a TWIC. Therefore, TSA is changing the waiver process to permit applicants who have been committed to a mental health facility or declared mentally incapable of handling their affairs to apply for a waiver. TSA will decide these waiver requests on a case-by-case basis. TSA will not necessarily require documentation showing that the disqualifying malady or condition is no longer present. The documentation submitted to TSA in support of the waiver request will be very important in making the waiver determination, however, applicants and/or their representatives should carefully consider and include all available information TSA can use to determine if the applicant poses a security threat.

8. TWIC Expiration and Renewal Periods

Several commenters stated that the TWIC should remain valid for more than five years. Most noted the cost of renewal as the basis for supporting a longer period. Commenters who supported a longer period also commonly argued that the biometric information, fingerprints, generally do not change over long periods of time. One commenter suggested requiring new fingerprints and digital photos only when something occurs to alter them significantly.

The NPRM proposed that a TWIC expire five years after it was issued, at the end of the month in which it was issued. *See* § 1572.21(e). In a new section, § 1572.23, the final rule retains this provision, except that the expiration occurs on the day, rather than end of the month, five years from when it was issued. Therefore, if a TWIC is issued March 20, 2007, it expires at the end of the day March 19, 2012.

As the technology and program mature, we plan to date the expiration of a renewal TWIC five years from the date the previous TWIC expired, so that applicants who begin the renewal process early are not penalized by having the initial 5-year term end early. We would like to provide a 6-month time period for renewal to give full opportunity to individuals to reapply in time to get a new TWIC before the old one expires, even if they are mariners that are away for long periods of time. A six-month time period would also encourage TWIC holders to apply early for renewal so that TSA has sufficient time for vetting of the applicant and to adjudicate an appeal or waiver, if appropriate, before the TWIC expires. However, the TWIC system programming cannot develop that capability by the time enrollment begins.

9. Fees for TWIC

Some commenters stated that the federal government should pay for some or the entire program. The law states that TSA must collect user fees in order to fund all program operations. The federal government has a statutory obligation, therefore, to collect fees in order to pay for program expenses.

Section 520 of the 2004 DHS Appropriations Act requires TSA to collect reasonable fees for providing credentialing and background investigations in the field of transportation. Fees may be collected to pay for the costs of the following: (1) conducting or obtaining a CHRC; (2) reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; (3) reviewing and adjudicating requests for waivers and appeals of TSA decisions; and (4) other costs related to performing the security threat assessment or the background records check, or providing the credential. 46 U.S.C. 469. Section 520 requires that any fee collected must be available only to pay for the costs incurred in providing services in connection with performing the security threat assessment or the background records check, or providing the credential. *Id.*

Some commenters said the fee was too high for dock, seasonal, and entry-level workers to pay because their income is low. TSA's fee authority, found in 6 U.S.C. 469, does not authorize TSA to adjust a fee based on the income of the applicant. Rather, Congress requires TSA to set a fee in amounts that are reasonably related to the costs of providing services.

Many commenters were concerned about an applicant having to pay multiple fees for background checks under other programs, such as HMEs. Another commenter stated that industry had already paid for modification and sustaining TSA's Screening Gateway in the HME program, and is essentially paying twice for the Screening Gateway under TWIC. TSA has addressed these concerns in the final rule by reducing the Card Production/Security Threat Assessment Segment for applicants who have already received a comparable threat assessment from DHS, including those for credentialed merchant mariners, HMEs, and FAST card holders.

Other commenters stated that the cost of card production and issuance fees should be separated from the information collection and threat assessment expenses. These commenters recommended that the applicant should only be required to pay for the services used: information collection and threat assessment. According to these commenters, TSA, not applicants, should fund the TSA infrastructure costs of card production, issuance and program management. Similarly, some commenters stated that only the persons who request an appeal or waiver should pay for the cost of adjudicating the security threat assessments and administering the appeal and waiver processes.

TSA agrees that costs should be segregated when possible, and has

worked to segregate costs depending on the service provided. For example, the TSA agent will collect a fee for the services provided by its trusted agents to enroll applicants, and the services to issue replacement cards. TSA will collect a fee for the background investigations only to the extent that it conducts new investigations. TSA will collect the FBI fee only from applicants that will be subject to a fingerprint-based CHRC, not from applicants who already have undergone a comparable CHRC. Congress granted TSA broad fee authority to collect a fee for ''providing the credential,'' and ''any other costs related to providing the credential or performing the background record checks.'' This includes the costs of card production, issuance, and program management. 6 U.S.C. 469(1), (3). Moreover, sec. 469(3) specifically requires TSA to collect a fee for reviewing and adjudicating requests for appeals and waivers.

Commenters were also concerned that fees collected would exceed the cost of implementing the system. However, under OMB guidance on user charges, TSA may charge fees only as sufficient to recover the full cost of providing the product and operating the program, and TSA has worked hard to estimate the costs of the TWIC program as accurately as possible. TSA's analyses of the appropriate costs that make up the fees in this rule include only the costs allowable by law and OMB guidance. OMB Circular A–25.

TWIC credentials will contain numerous complex technologies to make them secure and tamper-proof. The process for obtaining a TWIC is designed to ensure that the identity of each TWIC holder has been verified; that a threat assessment has been completed on that identity; and that each credential issued is positively linked to the rightful holder through the use of biometric technology. There are also significant operational costs associated with the TSA system and program support costs.

Pursuant to the Chief Financial Officers Act of 1990, TSA is required to review these fees no less than every two years. 31 U.S.C. 902(a)(8). Upon review, if it is found that the fees are either too high (*i.e.,* total fees exceed the total cost to provide the services) or too low (*i.e.,* total fees do not cover the total costs to provide the services), the fee will be adjusted. In addition, TSA may increase or decrease the fees described in this regulation for inflation following publication of the final rule. If TSA increases or decreases the fees for this reason, TSA will publish a Notice in the **Federal Register** notifying the public of the change.

Some commenters stated that the fee structure would require companies to pay for a TWIC card for a high volume of seasonal workers who may be gone before their cards are issued. Other commenters were concerned that a diverse range of ''casual'' laborers, such as plumbers, office cleaning crews, vehicle mechanics, utility repairmen, entertainers, and caterers, were omitted from the TWIC population used to calculate fees. These commenters stated that having to escort so many casual laborers into secure areas was impractical and a ''hidden cost.''

TSA derived its population estimate by determining which port workers would be most likely to need unescorted access to secure areas on a regular basis, and therefore, most likely to need a TWIC. TSA estimates that during initial rollout of the program, it will issue TWICs to approximately 770,000 workers who require unescorted access to secure areas of MTSA-regulated facilities. This approach is the product of survey and analysis work by TSA and Coast Guard personnel, using information provided by individual ports, public and private-sector data sources, interviews with sector subject-matter experts, and extrapolation from survey responses. An electrician who comes to the facility two times a year and other ''casual'' laborers may reasonably be escorted in the secure areas and thus may not need obtain a TWIC. Such workers were, therefore, not included in the population estimates.

The final rule requires vessels, facilities, and OCS facilities to escort individuals who do not hold TWICs and enter secure areas. The preamble now provides affected entities with more guidance on how to comply with this provision and the Coast Guard plans to issue a NVIC after publication of the final rule to provide even more clarity on acceptable escort standards. The language in the preamble states that within non-restricted secure areas, operators may simply monitor individuals without TWICs, while they must accompany individuals without TWICs in restricted areas. We anticipate that this guidance will provide operators with more understanding of the requirement, and perhaps more flexibility in implementing it.

Furthermore, we have included two new provisions that may reduce the economic burden of the requirement to provide escorts to individuals without TWICs. First, the final rule will allow facilities to submit to the Coast Guard amendments to their security plans in order to redefine secure areas. If facilities are able to redefine their secure areas in such a way as to focus on highly sensitive areas, and thereby limit the number of individuals who must enter them, then that may limit the costs associated with this requirement.

Second, the final rule allows passenger vessels and ferries to establish employee access areas that are neither public access areas nor secure areas. In these areas employees will be able to work unescorted without a TWIC. We believe that the final rule provides vessels, facilities, and OCS facilities with enough flexibility to accommodate the many of the temporary workers that are prevalent in the maritime industry.

Commenters inquired as to whether lifecycle costs such as yearly maintenance, card management systems, enrollment equipment and PKI certifications were included in the fee assessment. TSA's cost model does include the 5-year life cycle of the TWIC card and the associated costs of that life cycle.

One commenter stated that some applicants will not have credit cards or bank accounts, and that TSA should accept cash. TSA is concerned that the acceptance of cash would introduce problems concerning an audit trail and the potential for fraud. Therefore, the rule requires payment by cashier's check, credit card, or money order. If an applicant does not have a credit card or bank account, he or she can obtain a money order to pay the fee.

10. Implementing TWIC in Other Modes

The NPRM stated that TSA was considering requiring a TWIC in other modes of transportation, and invited comments. Several commenters supported this expansion. Such requests included coordination with other agencies to avoid negatively affecting mariners in later rule making processes, completion of a cost/benefit analysis to other transportation sectors, and insurance of the accurate, efficient, and reliable function of the TWIC in the maritime sector before extension to other transportation sectors. Several commenters urged that TWIC be used as a single biometric card and a single background check for the entire transportation sector. Commenters stated that duplicative credentials and clearances will still be needed because the proposed TWIC is limited to the maritime sector. A commenter noted that access control procedures may or may not differ across port facilities, airport, rail yards, and other facilities and suggested TSA invite comment on this matter.

Other commenters opposed expansion of the use of TWIC, citing burdens to industry, difficulty in translating to other transportation industries, and potential undermining of effective programs already in place. One commenter specifically opposed expansion of the TWIC program, noting that implementation problems and redundant regulatory requirements would significantly impact the propane industry. Some commenters noted that the TWIC program would create a competitive disadvantage for companies that chose to ship products via vessel versus companies with the same products that ship via air or ground. One commenter noted that current law requires a longer look-back frame for airport workers than the TWIC mandates, which would require a change in the law should TWIC be expanded to airport workers.

While TWIC will not supplant all other credentialing or background check requirements, we are working toward reducing the redundancy in background checks to the extent practicable. For instance, the threat assessment requirements for commercial drivers who hold an HME under 49 CFR part 1572 were originally designed to comply with MTSA and to be identical to the requirements for a TWIC. Under this rule, drivers who have completed TSA's security threat assessment for an HME are not be required to undergo a new threat assessment for TWIC until their HME threat assessment expires. These drivers will be required to provide a biometric for use on the TWIC and pay for enrollment services, credential costs, and appropriate program support costs. Similarly, individuals who have a FAST card issued by CBP will not be required to undergo another security threat assessment. *See* 49 CFR 1572.5(e). In addition, Canadian and Mexican drivers who haul hazardous materials and who are required to have a background check similar to that required for U.S. drivers may obtain a TWIC in order to meet that requirement. *See* 49 CFR 1572.201.

In the future TSA may conduct additional rulemaking to incorporate TWIC requirements into other modes of transportation.

D. Comments Related to Economic Issues

In order to evaluate the impact of the proposed rule, TSA and the Coast Guard published a Regulatory Impact Assessment (RIA) in May 2006 in support of the TWIC NPRM. The RIA was posted to the public docket and we received public comments that addressed many aspects of the assessment.

The majority of commenters discussed what they believe to be deficiencies or inaccuracies in our assessment. Several commenters, including individuals, businesses, government entities, and maritime trade associations, questioned some of the analytical assumptions we used to generate the cost estimates for the NPRM. In some instances, we agreed with comments, and used the information contained in them to refine the estimates for the RIA for the final rule. In other cases, we did not concur with comments on the RIA, and therefore did not use the assertions or claims in these comments to modify the assessment completed for the final rule. All comments on the original RIA were considered as part of this rulemaking effort, and have been summarized and responded to below.

1. Whether the Benefits of the Rule Justify the Costs

Although we received many comments to the public docket that supported the security goals of the rule, many individuals and businesses cited the potentially large economic impact of the rule and stated that the costs of the rulemaking action far outweigh the benefits. Individuals and firms from various segments of the maritime transportation industry, including the passenger vessel industry, the offshore marine service industry, the inland towing industry, and others, echoed this sentiment.

Many affected entities, especially operators on the inland waterways and small businesses, advanced a similar line of reasoning, arguing that there is not enough of a security risk to their operations to justify the measures we proposed.

We understand that the compliance costs of the rule represent a significant investment in security for many individuals and businesses. We do not dispute that the final rule may in fact impose considerable costs on many affected entities, including small businesses. As part of the economic analysis required by E.O. 12866, we have made every attempt to include all known costs in the RIA.

We also firmly believe, however, that the benefit of increased security to the U.S. maritime sector warrants the costs of the rule. The vessels, facilities, and OCS facilities affected by this rule represent some of the most important maritime and transportation infrastructure in the United States. Any vessel, facility or OCS facility that is regulated under 33 CFR subchapter H presents a risk of being a target of a transportation security incident, regardless of size and location, as determined by the interim final rule published by the Coast Guard in 2003 (July 1, 2003, 68 FR 39243).

In addition to claiming that the costs of the rule do not justify the benefits, some commenters stated that it is difficult to identify any solid benefits of the proposed rule. Some commenters alleged that the benefits outlined in the NPRM and the RIA were too vague. In particular, many, including the Office of Advocacy of the U.S. Small Business Administration (SBA Office of Advocacy or Advocacy) felt that the claim made by TSA and Coast Guard that the rule would streamline commerce was not well supported in the RIA, especially in light of the potentially high cost of the rule.

The primary benefit of the final rule is increased security to vessels, facilities, and OCS facilities covered under 33 CFR subchapter H. Under the final rule, individuals with unescorted access to secure areas of affected maritime establishments must undergo a security threat assessment and obtain a TWIC—a secure, biometric identification credential—that vessel and facility owners/operators will use to make access control decisions. The Coast Guard will conduct random spot checks of individuals' credentials.

The security threat assessments included in the rule will increase security at vessels and facilities by identifying individuals with dangerous criminal histories and potential ties to terrorism. And the secure, biometric credentials that will be issued under the final rule will allow owners/operators and the Coast Guard to verify that individuals with unescorted access to secure areas have in fact obtained a security threat assessment. Furthermore, even without card readers, TWIC provides greater reliability than existing systems because it presents a uniform appearance with embedded features on the face of the credential that make it difficult to forge or alter. We believe these benefits, in addition to the other security benefits described elsewhere, more than justify the costs of this rule.

In response to many comments received, we have revised the benefits section of the RIA for the final rule. Originally, the RIA for the NPRM stated that the proposal would enhance the flow of commerce by streamlining the number of credentials and access control procedures at U.S. seaports, eliminating the need for several port credentialing offices and systems, and creating an interoperable credential recognizable across the maritime

transportation environment. In their comments, many firms and individuals questioned the validity of these claims and provided specific examples that contradicted our assertions that the rule would facilitate certain business transactions.

We found these arguments compelling enough to remove the benefits to commerce that we originally included in the RIA that we published with the NPRM. After additional analysis, we agree with individuals and firms who questioned the benefits to commerce afforded by the rule. We firmly believe that the rule still has significant security benefits, a description of which still remains in the RIA.

A number of commenters, including Advocacy, referring to MTSA, stated that the law requires transportation security cards, not smart card readers, and that the benefits associated with these requirements do not justify the costs. Individuals and firms representing many sectors of the maritime transportation industry suggested that the requirements in the May 2006 proposal, including the card reader requirements, exceeded the statutory authority of TSA and the Coast Guard.

MTSA provides that DHS must issue biometric transportation security cards and ''prescribe regulations to prevent an individual from entering'' a secure area of a vessel or facility ''unless the individual holds a transportation security card'' or ''is accompanied by another individual who holds a transportation security card.'' 46 U.S.C. 70105(a). It is difficult to conceive of a cost-effective method to satisfy this section of MTSA that does not require an access control device to read the biometric credential. Even assuming an argument can be made successfully that MTSA does not authorize or require the use of biometric smart card readers, TSA and the Coast Guard have broad statutory authority to assess and regulate security in the national transportation system. We believe that the provisions originally proposed in the NPRM, including the card reader requirements, fall well within the statutory authority vested in both agencies by Congress.

As noted elsewhere, however, card reader requirements will be deferred until the readers have been piloted at 5 locations, and the public has had another opportunity to comment, as per the SAFE Port Act. As explained in other parts of this document, TSA and the Coast Guard will address technology requirements in a subsequent notice in the **Federal Register**.

2. Underestimated Compliance Costs

A number of commenters felt that several of the compliance costs estimated in the RIA for the NPRM were understated. Many firms, individuals, and trade associations that commented on compliance cost estimates expressed similar concerns. These concerns are summarized and responded to below.

(a). Biometric Smart Card Reader and Internet Connectivity Costs

Several commenters stated that the cost estimates in the RIA underestimated the expense of purchasing, installing, and maintaining biometric smart card readers. Industry commenters, including facility owners/operators who participated in the TWIC Phase III Prototype, asserted that the hourly wage rates used to develop installation costs were significantly understated, as were costs for maintaining and replacing sensitive electronic equipment that tends to degrade quickly in the marine environment. Other commenters, including the SBA Office of Advocacy, expressed concerns over the availability and reliability of card reader technology. Furthermore, many commenters declared that the cost of internet connectivity necessary to comply with the rule as proposed in the NPRM was excluded from the RIA.

Although we appreciate all comments on our analytical assumptions and cost estimates, these particular comments are no longer germane to this rulemaking because we have removed card reader requirements from the final rule. Therefore, we have also removed all card reader cost estimates from the RIA.

(b). Integration With Legacy Systems

One commenter asserted that the technical requirements included in the NPRM presented serious challenges for other affected government entities, which may have existing access control systems. This commenter claimed that TSA and the Coast Guard did not consider the integration of TWIC with other requirements, such as port authorities that operate mass transit systems or airports, in the cost estimates in the RIA. The commenter went on to state that these agencies may potentially be required to replace large legacy systems to incorporate the TWIC, and to maintain internal consistency and eliminate the expensive redundancy associated with credentialing their workers.

We realize that some affected establishments, both publicly and privately owned, have legacy systems that may need to be replaced or modified to incorporate the TWIC process. However, most of the costs would be associated with biometric readers. Since the requirement for biometric smart card readers has been removed from this final rule, these comments no longer pertain to this rulemaking. As stated earlier, TSA and the Coast Guard will address these issues at a later time. At that time, we will reevaluate estimates, including the cost for vessel and facility owners/operators to integrate new requirements with legacy systems.

(c). Administrative and Recordkeeping Costs

Several commenters stated that we greatly underestimated the administrative and recordkeeping burdens associated with the rule as proposed in the May 2006 NPRM. Citing what they perceived to be an onerous requirement to keep ongoing records of individuals accessing secure areas, many firms and individuals felt the estimates for the recordkeeping provision to be too low.

Moreover, many comments received from industry viewed the cost associated with developing the TWIC addenda to vessel and facility security plans as understated. In discussing the requirement that vessel and facility owners/operators must submit TWIC addenda to their security plans, many in industry opined that this task would involve several days of analysis that was not accounted for in the RIA for the NPRM.

The final rule will not require the recordkeeping measures or TWIC addenda as proposed in the NPRM. As a result, we have removed the estimated cost of these requirements from the RIA for the final rule. If we include these requirements in a future rulemaking, we will reevaluate the cost estimates included in the RIA for the NPRM.

(d). Opportunity Costs of Travel to Enrollment Centers

Many individuals and firms stated that the travel time estimate included in the RIA was too low, thereby underestimating the opportunity cost of traveling to and from TWIC enrollment centers. In their comments, individuals and firms provided time estimates for employees to travel to enrollment centers that ranged anywhere from three hours to several days.

Commenters who live in remote locations, such as Southeast Alaska, were particularly concerned that the estimate in the RIA did not accurately represent the cost to industry. In fact, some individuals and firms provided cost estimates for employee travel that

included estimated air fares, hotel expenses, and per diem allowances.

We partially agree with these comments. Given the uncertainty about the specific locations of enrollment centers and where affected individuals work and live, it was extremely difficult to estimate the amount of time it would take affected individuals to travel to and from TWIC enrollment centers. Furthermore, without information of this nature, we could not determine many costs associated with air or land travel (*i.e.*, air fares, cost of driving a privately owned vehicle, per diem allowances, etc.). For this reason, we excluded these costs from the RIA published with the NPRM, and conducted a different analysis to estimate costs.

To calculate the opportunity cost estimate included in the RIA for the NPRM, we assumed it would take an individual, on average, one and one half hours to complete enrollment. In attempting to calculate this time estimate, we divided the total time necessary to enroll into three components: (1) Travel time; (2) enrollment time; and (3) wait time.

To forecast total travel time, we used an estimate from the Department of Transportation on the average commute time for individuals traveling to work in privately owned vehicles, the primary means of transportation for commuters in the United States. Although clearly not a perfect measure of travel time to a TWIC enrollment center (due to lack of information outlined above), this estimate was 22.49 minutes for a one-way trip. In our total time estimate, we multiplied this number by a factor of two in order to account for travel both to and from an enrollment center.

In order to account for the time needed for workers to enroll at the TWIC enrollment centers, we used data collected by TSA during the TWIC Phase III Prototype on the average amount of time per enrollment. This time estimate was 10.35 minutes.

Finally, we added 30 minutes to the time estimates described above to provide for possible wait time at the enrollment center and other incidental events. These estimates, collectively, gave us an approximate total time estimate of 90 minutes, which we in turn used to calculate the opportunity costs of this requirement. We used this time estimate to calculate the opportunity cost of credential issuance, too.

We acknowledge that this time estimate may have led us to understate the opportunity costs of this provision. For example, individuals living in remote areas may have to travel long distances in order to enroll in the program. (TSA and the Coast Guard note, however, that there may be other individuals who live and work near enrollment centers and may complete the process in less than 90 minutes.)

Although we acknowledge that our calculation of opportunity costs in the NPRM may have underestimated the burden to some employees and employers, we have found it difficult to generate a more credible point estimate for this cost element. Some individual commenters provided us with anecdotal data on the amount of time it would take them to travel to TWIC enrollment centers, with estimates ranging from several hours to multiple days.

However, given the fact that the final enrollment center locations were not published before the end of the comment period, we do not know how these individuals calculated their estimates. Furthermore, we believe that many of the comments submitted on this matter came from individuals who reside the furthest from major seaports and cities. Most enrollment centers are likely to be located in major seaport areas, where the majority of the affected population is likely to reside. In fact, TSA and the Coast Guard revised the original list of seaport communities slated to have an enrollment center after receiving helpful comments from various segments of the maritime industry.

In response to these comments and all of the uncertainty surrounding this time estimate, we decided to develop a range for our cost estimate for the final rule. After reading the many comments on this matter and reviewing our previous assumptions, we concluded that this methodology provided the best way for us to address industry concerns without severely over-or understating the cost of the provision.

To develop the range for this cost estimate, we used the time estimate of one and a half hours included in the NPRM as the lower bound and a time estimate of eight hours as our upper bound. We based the upper bound time estimate on comments received from individuals in the maritime sector. As a primary estimate, we used four hours, or half a work day. We believe this time estimate allowed us to calculate a more accurate estimate of the opportunity costs to individuals and industry. More discussion of this range can be found in the RIA accompanying this final rule.

(e). Cost of Lost Labor Due to Wait Time

Many commenters expressed concern that the amount of time to process a TWIC application would impede their ability to hire new employees. The NPRM preamble stated that facility and vessel owners/operators must notify workers of their responsibility to enroll and that generally, owners/operators should give individuals 60-days notice to begin the process. Many commenters objected to this timeframe, referring to it as a ''60-day waiting period.'' One commenter urged TSA to dedicate additional resources to ensure the system has the capacity to handle the processing load. Other commenters believed that completing the threat assessment in less than 30 days is optimistic.

These commenters also asserted that their operations would suffer as a result of this ''60-day waiting period,'' and that this cost was excluded from RIA. Still others asserted that the ''waiting period'' would encourage vessel owners/operators to operate in violation of the rule or force them to operate with insufficient crew, putting both employers and employees in danger.

Moreover, several commenters, including the SBA Office of Advocacy, discussed how the ''60-day waiting period'' for a new employee to receive a TWIC puts them at a particular disadvantage for attracting seasonal labor. Enterprises operating passenger vessels were particularly concerned about this ''waiting period,'' as they asserted it would make it difficult to hire employees during the summer months, which tend to be the busiest for them.

TSA and the Coast Guard recognize that having employees wait to obtain a TWIC before they can start work is burdensome for some businesses. We understand that businesses in the maritime sector, including large seaport terminal operators, depend heavily on temporary or ''casual'' workforces that are hired with little notice. Furthermore, TSA and the Coast Guard are sensitive to the needs of employers who primarily utilize seasonal labor to staff their facilities and vessels.

It is important to note, however, that TSA and the TWIC program do not have a ''waiting period,'' mandatory or otherwise. Rather, TSA must adjudicate the security threat assessment of each applicant following enrollment and each case necessarily entails processing time. As a general rule, security threat assessments and issuance of a TWIC should take no longer than 30 days. In fact, in TSA's experience completing threat assessments for commercial drivers with hazardous materials endorsements, threat assessments are typically completed in less than 10 days. However, processing time increases for an applicant with a criminal history or other disqualifying

information, and is further lengthened if the applicant initiates an appeal or waiver.

Nevertheless, to address this concern we have included in the final rule a provision that should allow employees to begin work before they receive a TWIC. First, newly hired individuals employed by affected firms can work in secure areas, including restricted areas, as long as they are escorted by an individual with a TWIC. The escort policy was proposed in the NPRM and remains in the final rule. This provision should allow many firms to make minimal adjustments to their current hiring practices, and allow many new hires to start work immediately.

The final rule also creates ''employee access areas,'' allowing passenger vessel and ferry owners/operators more flexibility in implementing the requirements of the rule. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not to passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the vessel security plan. We believe that this new provision should reduce the regulatory burden on many small passenger vessels, especially those that primarily utilize and rely on seasonal labor. In fact, we believe this new policy will exclude the vast majority of seasonal employees from even needing a TWIC.

The final rule also includes a new provision that will allow a direct hire new employee to receive limited access for 30 consecutive days to secure areas, including restricted areas, of a vessel or facility provided that the new employee passes a TSA name-based check. If TSA does not act upon a TWIC application within those 30 days, the cognizant Coast Guard COTP may further extend a new hire's access to secure areas for another 30 days. This new policy, which TSA and the Coast Guard developed as a result of comments on the NPRM, is intended to give owners/operators the flexibility to quickly grant new employees who do not yet hold a TWIC access to secure areas. In order to ensure ample security for vessels and facilities, though, there are certain requirements that owners/operators and TWIC applicants must meet under the new provision. These requirements are described elsewhere in this document and in the regulatory text.

By clarifying commenters' misconceptions regarding the ''waiting period,'' and including the new policies described above, we believe the final rule allays several concerns expressed by firms and individuals in the maritime sector. For this reason, we did not include additional cost estimates to account for lost labor attributable to the ''waiting period'' for a TWIC.

(f). Appeals and Waivers

One industry association expressed concern about the cost estimate TSA and Coast Guard included in the RIA for the NPRM to account for applicants to file appeals or waivers with TSA. In arguing that the cost estimate was understated, this association stated that the proposed rule only includes the time preparing correspondence, but a more accurate assessment would include lost wages while the application is being reconsidered.

Although an individual may not receive unescorted access to secure areas while awaiting the determination of an appeal or waiver request, there is nothing in the final rule that would prohibit such an individual from working in a secure area while under the supervision of a credentialed escort. For this reason, we did not include a cost estimate for lost wages while considering this requirement. TSA and the Coast Guard did, however, include cost estimates for employers to provide employees and visitors with escorted access in the RIA.

(g). Cost To Provide Real Estate to Enrollment Providers

A commenter stated that TSA and Coast Guard assume that port facilities will provide space and utilities for enrollment centers, but that the RIA does not account for the direct and opportunity costs for these facilities.

The NPRM did not propose, and the final rule does not require, maritime facilities to supply enrollment providers with space to conduct operations. We therefore did not include this cost in the RIA.

(h). Escorting Costs

Several commenters stated that TSA and the Coast Guard underestimated the cost of complying with the escorting requirements that were proposed in the NRPM. Commenters felt that the escorting requirement would be too burdensome in terms of manpower—several stated that they would need to hire additional personnel—and additional operating costs. Many commenters stated that TSA and the Coast Guard did not take into consideration temporary workforces utilized by many maritime facilities and vessels, which would require escorts when developing this provision. Furthermore, many of these commenters interpreted the definition to require the physical presence of one escort for each individual without a TWIC at all times while in a secure area. Some of these commenters provided examples of situations where the requirement would be too burdensome. For example, one port authority stated that it typically has over 100 temporary workers on site that would require escorts.

We agree with these comments, in part, in regard to the statement that the cost estimates for affected entities to comply with this provision of the rule may have been understated in the RIA. However, we also believe that many affected firms and individuals have misconceptions about what the provision requires of vessels, facilities, and OCS facilities.

As proposed in the NPRM, the escorting requirement is a performance standard rather than a strict definition. After analyzing many comments, we believe some affected individuals and firms may have misinterpreted our intent with respect to this requirement. Therefore, we recognize that some guidance is needed. As discussed elsewhere in this final rule, we expect that, when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, physical escort. Whether it must be a one-to-one escort, or whether there can be one escort for multiple persons, will depend on the specifics of each vessel and/or facility. The Coast Guard will provide additional guidance on what these specifics might be in a NVIC. Within non-restricted secure areas, however, such physical escorting is not required, as long as the method of surveillance or monitoring is sufficient to allow for a quick response should an individual ''under escort'' be observed in an area where he or she has not been authorized to go or is engaging in activities other than those for which escorted access was granted.

With this understanding of the requirement in mind, we estimated in the NPRM that maritime facilities would need 240 additional labor hours on an annual basis in order to comply with this requirement. We did not report compliance costs for this requirement for vessels or OCS facilities and in retrospect, we believe this was an oversight.

In attempting to estimate compliance costs for the NPRM and the final rule, we found that the uncertainty surrounding how affected entities would implement this requirement made it difficult for us to develop accurate compliance cost estimates. Further, the final rule contains several provisions aimed at providing affected entities with regulatory flexibility,

which increases the level of uncertainty in our analysis.

For example, facilities may now submit amendments to their security plans in order to redefine their secure areas to those portions of their facility involved in maritime transportation or at risk of a transportation security incident. By decreasing the size of their secure areas, firms could limit the number of individuals who need a TWIC, and also decrease their escorting compliance costs.

Also, the final rule creates ''employee access areas'' that, as described above, are defined spaces within the access control areas of ferries or passenger vessels that are open to employees but not to passengers. These areas are, by definition, not secure areas and do not require a TWIC for unescorted access. The areas may not include any areas defined as restricted areas in the vessel security plan. This provision, we believe, could provide flexibility to vessels that would otherwise incur high costs to provide employees with escorts.

The final rule also allows owners/operators to provide new employees with limited access to secure areas for 30 consecutive calendar days (and may be extended an additional 30 days at the discretion of the cognizant Coast Guard COTP). Although this provision, in an effort to balance security with commerce, contains certain restrictions, we believe it also may help to limit escorting costs associated with physical accompaniment within restricted areas.

Finally, the provision for passenger access areas, which we originally proposed in the NPRM for passenger vessels, remains in the final rule and provides flexibility for owners/operators offering marine services to passengers. MTSA requires that no one be given unescorted access to secure areas unless they carry a TWIC. To ensure that passenger vessels do not have to require passengers to obtain TWICs or escort passengers at all times while on the vessel, the rule creates the ''passenger access area,'' allowing vessel owners/operators to carve out areas within the secure areas aboard their vessels where passengers are free to move about unescorted. This should also reduce escorting costs.

We believe that the provisions listed above should give owners/operators flexibility to follow the requirements of the rule, including the escorting requirements, without causing undue economic harm. In particular, we believe the rule now allows for regulatory flexibility when it comes to ensuring that facilities and vessels can continue to utilize temporary workforces without incurring high compliance costs.

Even though the rule now provides flexibility for owners/operators with respect to the escorting requirement, we have decided to increase our initial compliance cost estimates for this provision. We concluded that our initial estimates, in light of the helpful comments we received during the public comment period for the NPRM, most likely understated the cost of complying with this provision. The new estimate for the final rule will include compliance costs for vessels and OCS facilities, which we excluded in the NPRM. We have also concluded that a range of compliance cost estimates for this requirement would be more appropriate than a single point estimate, given the several ways in which owners/operators can now minimize their risk of incurring high escorting costs. The adjusted cost estimates are described in more detail in the RIA.

(i). Costs for Redundant Credentials

One employer stated that it already paid fees for employees to obtain port identification credentials. In addition to the fees, the employer commented that it incurred costs while employees took time off from work to obtain the credentials. This commenter asserted that employees will continue to be issued their respective port identification credentials. For example, employees will have to register with all the ports they frequent and pay local administrative costs to be placed on additional port or terminal rosters. This commenter implied that the cost of this redundant process was not accounted for in the RIA.

We realize that the cost of compliance from port to port will vary and that there may be local requirements for personnel to obtain identification credentials other than the TWIC. Private firms are free to create their own credentialing systems and it is beyond the authority of TSA or the Coast Guard to preclude a private company from issuing its own identification card.

However, the TWIC is a unique credential in so far that it provides owners/operators with a means to confidently assess the risk posed by an individual seeking unescorted access to a secure area of a vessel or facility. The distinctive security threat assessment completed by TSA on each TWIC applicant is not replicated by other public sector (*e.g.*, port authorities) or private sector credential providers. Accordingly, we do not believe that the TWIC is a redundant credential. In the RIA for the final rule we have accounted for all costs associated with producing and issuing the TWIC. Additionally, we do not agree that all currently existing port credentials will continue to be required once TWICs are issued and being utilized. We believe that some port authorities and other providers of identifications will eliminate separate credentialing requirements and rely instead upon the TWIC and the security threat assessment done by TSA.

(j). Costs to Shipbuilders

An association of shipbuilders asserted that the NPRM represents a redundant regulatory burden for shipyards. The association noted that many shipyards already comply with DOD security plan regulations, and that these standards, in many instances, provide greater security than the provisions proposed in the NPRM. In its comment to the public docket, the association suggested that such shipyards should be exempt from the requirements of the rule.

Along with other individual shipbuilding companies, the association also expressed concern with several of the assumptions used in the cost estimates for the NPRM. In particular, the association articulated its concern about the population estimate—it stated that a conservative estimate for the number of affected individuals employed at the six shipyards that are members of this particular organization, which include vendors, shipyard employees, and contractors, would exceed 200,000.

In addition, this organization averred that the estimates for most direct and indirect costs of the rule were severely understated. Many of these costs would be pushed onto U.S. taxpayers in the form of higher costs for ships purchased by the U.S. government, including the Coast Guard.

TSA and the Coast Guard are aware that many shipyards must comply with Department of Defense security regulations that govern identification credentials, facility security plans, and other provisions intended to augment U.S. maritime security. However, we do not believe that this rule will affect all shipyards; therefore, we disagree that we have significantly underestimated the shipyard population.

If a shipyard falls within the applicability of the MTSA regulations and is required to submit a facility security plan under 46 U.S.C. 70105, then any individual requiring unescorted access to a secure area is required to have a TWIC. We note, however, that shipyards are specifically exempt from 33 CFR part 105 applicability (*see* 33 CFR 105.110(c)), and would only fall under the facility

security regulations if the shipyard is subject to a separate applicability requirement, such as being regulated under 33 CFR part 154, the oil/hazmat in bulk requirements.

For the reasons stated above, we do not believe that all shipyards will fall under the requirements of the final rule, and therefore disagree that the number of shipyard employees that would need to obtain a TWIC would exceed 200,000. In our population estimate, we calculated that 55,000 individuals working in this industry would initially be affected by the rule, and we continue to believe this is an accurate estimate. Moreover, outside of our shipyard population estimate, we included estimates for contractors/others and site management/administration, two population segments that most likely have some presence in U.S. shipyards.

With respect to understated or omitted cost estimates, TSA and the Coast Guard have made a number of changes to the final rule that should allay some of the concerns expressed by the shipbuilding industry and other shipbuilders. In the RIA for the final rule, we have also adjusted some assumptions and cost estimates to reflect comments received from various sectors of the maritime industry. We have discussed these changes elsewhere in this section and in the RIA. As for increased costs to the U.S. government, we did not have enough information to make a judgment on this assertion.

(k). Rule Will Exacerbate Industry Labor Shortages

Many commenters mentioned that the labor force in the maritime industry is strained, and that the requirements of the final rule, including the security threat assessment standards and user fees, will only intensify the problems associated with a tight labor market. Many firms, concerned about the fee requirements and the security threat assessment standards, believed the rule will give many prospective employees a disincentive to work in the maritime industry. Several commenters also noted that existing employees may not apply for a TWIC due to the security threat assessment.

TSA and the Coast Guard understand that many segments of the maritime transportation sector are experiencing labor shortages. We also believe, however, that the lack of capable employees in many areas of the maritime industry is a function of factors outside the control of TSA or the Coast Guard.

Nevertheless, the final rule may have an impact on some labor markets. TSA and the Coast Guard concur that some individuals—due to the user fees, security threat assessment standards, or other factors—may no longer seek employment at businesses regulated by 33 CFR subchapter H. Short of speculating on this effect, however, we have no way of quantifying the impact to labor markets. In our research, we found no data or information that would have allowed us to measure the potential effects on the labor market of the rule, and commenters did not provide specific data with respect to this issue.

To the extent possible, though, we have drafted the final rule so that it would not adversely affect the supply of labor in the maritime transportation sector. We needed to balance this effort, of course, with the primary security objectives of the rule. The following amendments to the final rule, we believe, will help ease the effect of the regulation on the labor supply:

- Expanding the group of non-U.S. citizens who meet the immigration standards to include foreign nationals who are students at the U.S. Merchant Marine Academy or comparable State school; commercial drivers licensed in Canada or Mexico transporting hazardous materials into and within the U.S.; citizens of Canada or Mexico who are in the United States to conduct business under a NAFTA visa; and a variety of professionals and specialists who work in the U.S. maritime industry on restricted visas;
- Enlarging the response time for applicants to appeal an adverse determination, correct an open criminal disposition, or apply for a waiver from 30 or 45 days to 60 days;
- Expanding the group of applicants eligible to apply for a waiver after being disqualified because of mental incapacity;
- Including a provision for passenger access areas, as proposed in the NPRM;
- Adding a provision for employee access areas on passenger vessels and ferries;
- Allowing facilities to submit amendments to their security plans in order to redefine their secure areas; and
- Allowing new employees who have applied for a TWIC to receive limited access to secure areas for 30 consecutive calendar days (which may be extended an additional 30 days by the cognizant Coast Guard COTP if TSA has not acted upon the TWIC application in the initial 30-day period).

TSA and the Coast Guard have concluded that these provisions both achieve greater security in the maritime sector and mitigate potential adverse impacts to affected labor markets.

(l). Rule Will Increase Congestion and Delays at Maritime Facilities

Some commenters stated that the rule would increase delays and congestion at port terminal access points across the country, thereby increasing logistics and shipping costs. One association representing large domestic and international carriers, as well as stevedores on the West Coast, stated that it was concerned about cargo backups, congestion fines, and late starts that may result from faulty access control system hardware or software that may not withstand the rigors of the marine environment. These costs, the association noted, were excluded from the RIA for the NPRM.

We agree with these commenters that costs associated with congestion, delay, and late starts were not included in the RIA for the NPRM. TSA and the Coast Guard understand that anything that impedes the efficient delivery of waterborne cargo may impose a cost on affected entities and the U.S. economy. At the time of publication of the NPRM, we did not have any data that would have allowed us to estimate the proposed rule's impact on the logistics of waterborne and inland cargo movement.

As stated above, the final rule will not require vessels, facilities, and OCS facilities to use the TWIC in concert with biometric smart card readers at access points. The rule instead mandates that all persons seeking unescorted access to secure areas must present their TWIC for inspection before being granted unescorted access.

Individuals seeking unescorted access to vessels, facilities, and OCS facilities are currently required to show a form of identification as stipulated by 33 CFR subchapter H. Since the final rule requirement simply replaces the current acceptable identification with a TWIC, the rule should not cause any significant delays at facilities or other locations in the maritime transportation sector. Random checks of credentials conducted by the Coast Guard are not expected to cause delays. Furthermore, this change to the proposed rule should not require facilities to establish covered pull-over lanes for trucks seeking to enter their secure areas, as suggested by some commenters. For these reasons, we have excluded these costs from the RIA for the final rule.

(m). Decreased Competitiveness of Regulated Firms

Some firms that deal in international markets stated that they would be at a unique disadvantage under the rule while attempting to compete with

foreign businesses. This theme was presented by international ferries in the Pacific Northwest and repeated by offshore supply vessels operating in the Gulf of Mexico.

Firms that deal solely domestically also commented that the rule would hamper their efforts to compete in markets occupied by businesses not regulated by 33 CFR Subchapter H. Both groups of commenters asserted that TSA and the Coast Guard failed to account for this decrease in competitiveness and corresponding costs in the RIA.

In some markets, the cost of compliance with the final rule may raise some firms' operating expenses and therefore impede their ability to successfully compete with foreign or domestic competitors not subject to the rule. We believe, as previously stated, that the costs are justified by the increased level of security provided by rule. Without data or other information about this potential effect, we could not quantitatively measure it.

However, we also believe that the final rule includes provisions, especially for passenger vessels and ferries, which should allay commenters' concerns about compliance costs and competitiveness. As stated above, new provisions for passenger access areas, employee access areas, and new employees may decrease compliance costs. Also, for certain facilities, the ability to redefine secure areas may decrease the costs of complying with the rule.

International ferries stated that they are suffering from regulatory exhaustion and cannot pass regulatory compliance costs onto their customers.

As stated above, we understand that this rule may impose significant impacts on ferry operators. We have attempted to estimate these impacts to the best of our ability. The final rule contains new provisions that should provide passenger vessels, including ferries, with some flexibility in complying with the rule. This regulatory flexibility may also decrease compliance costs for affected firms.

The provisions for employee and passenger access areas, as described above, were designed to help passenger vessels, including ferries. Also, the provision that allows new employees to receive limited access to secure areas for 30 consecutive days should also decrease concerns about adverse impacts on firms that use seasonal employees.

Commenters from the passenger vessel industry stated that costs would decrease their competitiveness because they are competing against non-marine companies that would not incur regulatory costs. This industry also noted its reliance on seasonal hires may put it at a unique disadvantage when trying to attract labor.

TSA and the Coast Guard recognize that firms in the passenger vessel industry will incur costs under the final rule that some of their competitors may not incur, and that this may decrease their competitiveness. To the best of our ability, we have attempted to accurately estimate compliance costs to all affected entities. However, lack of data on unique markets and firms has made it impossible for us to predict any effects on competitiveness.

We also realize that this final rule presents unique challenges for industries that rely predominately on seasonal workers. As discussed in this section, TSA and Coast Guard have included provisions in the final rule to give these industries flexibility in complying with the rule. For example, the final rule allows ferries and passenger vessels to designate employee and passenger access areas. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open only to employees whose employment is solely related to passenger service and/or entertainment. It is not a secure area and does not require a TWIC for unescorted access. Passenger access areas were created to ensure that passenger vessels do not have to require passengers to obtain TWICs or escort passengers at all times while on the vessel.

Furthermore, affected entities will now be allowed to give new employees limited access to secure areas for 30 consecutive days, provided the employees have applied for a TWIC and meet the provision outlined in more detail in the regulatory text. This may be extended an additional 30 days by the cognizant Coast Guard COTP if TSA does not act upon the individual's TWIC application within the original 30 days. We believe these provisions will help employers that utilize seasonal employees.

(n). Increased Prices for Consumer and Producer Goods and Service

Some commenters asserted that the rule would increase the price of goods moved by firms in the maritime transportation sector, and that this cost was excluded from the RIA.

Although we think this effect is highly unlikely given the amount of competition in the transportation marketplace, we agree that it could happen in some markets because transportation costs can affect wholesale and retail prices. However, many other factors, such as consumer demand, also affect prices. Commenters did not provide detailed data on specific goods and markets. Due to lack of data on individual markets, we did not attempt to quantify this effect in the RIA for the final rule.

Another commenter stated that the costs of the rule will extend to security personnel and other contractors, who will pass this cost on to their customers, and that this cost was excluded from the RIA.

As stated above, we realize that the cost of compliance may be passed on to customers in some markets. However, prices for goods and services are determined by myriad factors, including factors other than firms' operating costs.

Regulated vessels, facilities and OCS facilities operate in a number of markets and we could not determine which firms would be able to pass compliance costs on to customers. We therefore did not attempt to quantify this potential effect in the RIA.

(o). Additional Recruiting Costs

Many employers commented that the rule would increase their hiring costs and that this burden was excluded from the RIA. For example, some firms noted that they would need to pay application fees for prospective employees and that they might have to offer more incentives to attract new staff members.

TSA and Coast Guard agree that employers in markets where the supply of labor is very tight may incur some additional hiring costs. For example, some employers may find that they will have to pay the TWIC user fees for new employees. In other industries, however, this may not be true. Due to this uncertainty, we did not quantify this potential burden to employers in the RIA.

(p). Decreased Productivity

Some commenters asserted that the rule would decrease employee and employer productivity and that this cost was not included in the cost estimates in the RIA. Specifically, one commenter stated that the rule would impose a negative, one time productivity shock on the maritime industry while firms and individuals adjust to new access control procedures and other requirements.

Although we concur that some firms could suffer decreased productivity under the rule, we encountered difficulty when trying to gauge this potential effect of the rule on affected vessels, facilities and OCS facilities. Even though some commenters claimed productivity would suffer as a result of the rule, we did not receive any quantitative estimates of this effect;

therefore, we did not attempt to quantify this impact in the RIA for the final rule.

Moreover, we believe that industry commenters were most concerned about the effect on productivity that would result from profound changes to many current physical access control systems (*i.e.*, smart card readers) that would have been necessary under the requirements of the NPRM. Because this final rule does not require smart card readers, this concern should be mitigated to some extent.

2. Economic Impact of Secure Area Definition

The SBA Office of Advocacy, as well as several other commenters noted that TWIC may be a costly rule for the maritime industry to absorb. In particular, many facilities noted that the costs of the rule are largely driven by the secure area definition. Some facilities were confused about this definition and requested more guidance.

As stated above, we understand that there is some confusion about the definition of a secure area. A secure area is now defined in the final rule as the area onboard a vessel or at a facility or OCS facility over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard approved security plan. It does not include passenger access areas, employee access areas, or public access areas, as those terms are defined in §§ 104.106, 104.107, and 105.106, respectively, of 33 CFR subchapter H. Facilities subject to part 105 of this subchapter may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident. We believe the final rule now provides a clear definition of secure area and that it affords facilities with some flexibility that may ultimately decrease compliance costs.

3. Economic Impact of TWIC User Fees

(a). Fees Are Too High and Will Adversely Impact Employees in the Maritime Industry

Many commenters asserted that the user fees proposed in the NPRM would negatively impact already financially strapped individuals in the maritime workforce. Employers in particular were concerned about individuals' ability to pay the fees, and the effect this could have on the labor force.

We understand that the fees associated with the credential represent a significant investment in security for many individuals and/or businesses. Furthermore, the opportunity cost for individuals to travel to and from enrollment centers also represents a cost to industry and individuals.

The fees associated with obtaining a TWIC represent the cost to TSA of providing all services—including enrollment, security threat assessments, issuance, and the TSA system—related to the credential. TSA cannot meet its statutory mandate without delivering these services, and it cannot deliver these services without collecting user fees. By law, TSA is responsible for collecting user fees to cover the costs of all TWIC program operations. Section 520 of the 2004 DHS Appropriations Act requires TSA to collect reasonable fees for providing credentialing and background investigations in the field of transportation.

During the course of the rulemaking, we contemplated giving a discount on certain fees to employees working at small businesses and other subsets of the population. After careful analysis, we determined that this would not be feasible. First, TSA's fee authority found in 6 U.S.C. 469 does not authorize TSA to adjust a fee based on the income of the applicant. Second, it would be difficult for TSA and the Coast Guard to credibly distinguish individuals working in different segments of the industry.

Where possible, we have made provisions in the rule to ensure that individuals do not pay for redundant criminal history records checks. Furthermore, TSA and the Coast Guard have made every effort to ensure that the fees only cover the cost to TSA of delivering program services. In an effort to make certain that the level of user fees collected by TSA does not exceed the total costs of the program, TSA and the Coast Guard, pursuant to the Chief Financial Officers Act of 1990 (31 U.S.C. 902(a)(8)) will review fees at least every two years.

In addition to taking these steps, the Coast Guard is proposing to combine the number of credentials that mariners are required to carry under Title 46 of the CFR, and to remove the requirement for mariners to travel to a Regional Examination Center (REC). This would reduce the financial burden to mariners as they would only be required to pay one application fee of $45. Mariners would no longer be required to travel to one of 17 RECs unless they need to actually sit for an exam. This would bring significant savings to this population, as many mariners currently have to travel long distances to attain their seafaring credentials.

(b). Responsibility for Credential User Fees and Compliance Costs of the Rule

A number of commenters stated that the Federal government should pay for some portion of the program. In their comments, many firms and individuals noted that the goal of increased security in the United States is a common one, shared broadly by individuals in all parts of the country, and that the cost of providing such security should be borne by all U.S. taxpayers.

As stated above, the law states that TSA must collect user fees in order to fund all program operations. The Federal government has a statutory obligation, therefore, to recover program expenses through fees.

Commenters stated that employers, not applicants, would bear the cost of TWIC user fees. Many industry trade associations and individuals businesses asserted that many employees, especially those with lower incomes, would rather work in other industries than pay the user fees. The burden of covering such fees, therefore, would fall on employers.

TSA and the Coast Guard agree that some employers may pay the TWIC user fees for their employees, although this is not a requirement of the rule. Unfortunately, we have no way of knowing which companies will have to bear the cost of obtaining a TWIC and which companies will require their employees to absorb the cost. Commenters did not provide specific data to substantiate the claim that employees would seek work in other industries rather than pay the fee to obtain a TWIC. Therefore, we did not attempt to estimate this distributional impact in the RIA for the final rule, although we did account for the total cost of this provision.

4. Comments on Estimated Population

(a). Analysis Omitted Populations

Several commenters stated that TSA and the Coast Guard omitted several maritime populations in the RIA for the NPRM. Specifically, a trade association representing U.S. port authorities stated that many port operations rely on temporary workforces, and that many casual laborers are given visitor or temporary passes to allow access. This commenter claimed the size of this casual labor force can be significant. It is concerned about their omission in the rule and questions how much consideration TSA and the Coast Guard gave to these workers. The trade association also noted that while these workers are usually supervised to a certain degree, the proposed rule would

likely still require them to obtain a TWIC or a credentialed escort.

As previously stated in this section, TSA and the Coast Guard believe that the final rule provides enough flexibility to allow business owners to accommodate temporary workers without incurring high costs. Certain facilities operating in the maritime environment will be allowed to submit amendments to their security plans in order to redefine their secure areas. We also believe, as the trade association alluded to in its comment, that many of the individuals in the casual workforce usually receive some sort of oversight during their time of employment in the maritime industry. Although circumstances are unique to each facility and vessel, TSA and Coast Guard believe that many operations, while employing ''casuals'' may already meet the escort requirement of the final rule while employing casuals. This would preclude these individuals from having to obtain a TWIC. For this reason, we did not adjust the population estimate included in the RIA to account for additional temporary workers.

The Edison Electric Institute, the American Public Power Association, and the National Rural Electric Cooperation Association commented that TSA does not appear to have included the 30,000 utility employees who could be subject to the rule. Furthermore, they stated that utilities generally are not in the business of transportation and therefore should not be subject to the rule.

TSA and the Coast Guard recognize that certain facilities regulated by 33 CFR part 105 may have only a small nexus to transportation. For this reason, we have included in the final rule a provision to allow facilities to submit amendments to their security plans that would allow them to adjust the definitions of their secure areas. This would ensure robust security within sensitive transportation areas. For this reason, we did not adjust our population estimate to include employees in the utilities industry.

The requirement that all individuals needing unescorted access to secure areas of 33 CFR subchapter H-regulated facilities would bring into the nexus of transportation workers a plethora of individuals that some commenters believe TSA has not properly accounted for in its estimate of 750,000 affected individuals.

One particular trade association representing the fertilizer industry anticipates delivery personnel, such as Federal Express, United Parcel Service, and the United States Postal Service employees; general contractors, such as plumbers, vehicle mechanics, builders; chemical distributors; college interns; office cleaning crews; food service personnel; utility repairmen and utility/pipeline personnel with right-of-way on facility property to require intermittent access to secure areas of regulated facilities. Because the amount of personnel needing access to a facility is well beyond the nexus of transportation that TSA and the Coast Guard account for in the NPRM, this trade association believes the population estimate needs to be re-examined and proposed again for review as an NPRM.

We fully understand that a number of individuals working in a wide array of occupations would be affected by the final rule. While conducting research to formulate the estimated population, TSA and the Coast Guard examined a number of industries that provide services to affected vessels, facilities, and OCS facilities, such as general contractors, delivery personnel and the like.

In the population estimate included in the RIA for the NPRM, TSA and the Coast Guard estimated that the rule would impact 70,000 contractors and other personnel in the maritime industry. We believe that the occupations listed above by the commenter are included in this estimate; therefore, we did not change the population for the final rule in response to this comment.

One commenter asserted that the rule has an overly expansive scope that is unrelated to the actual risk posed by certain personnel, such as grain elevator personnel, truck drivers and rail carriers delivering inbound grain.

TSA and the Coast Guard firmly believe that all vessels, facilities, and OCS facilities covered by 33 CFR subchapter H are critical maritime assets that are at some risk of being involved in a transportation security incident. Therefore, we believe all personnel with unescorted access to secure areas of these regulated entities should receive a security threat assessment and a TWIC.

An association representing passenger vessels stated that there are probably tens of thousands of vessel wait staff, entertainers, supporters, suppliers, caterers and other persons, who are not identified in the population estimate in the RIA.

We agree with this particular association that some of the entertainers, caterers, and wait staff employed in the passenger vessel industry were most likely not captured in our population estimate in the RIA for the NPRM. This is because we intended for the ''passenger access area'' provision, included in the NPRM, to cover these individuals. Upon reviewing the comments, we determined that many of these individuals would need access to additional areas of the vessel that are not open to passengers and therefore not covered by the ''passenger access provision.'' However, rather than add them in to the population estimate, we added the ''employee access area'' provision, which should preclude entertainers and wait staff, as well as other personnel with only a tangential connection to transportation, from having to obtain a TWIC.

The categories of personnel as ''contractor/other'' and ''vessel operation/port support,'' which are included in the population estimate, likely include the other personnel mentioned by this association, namely the supporters and suppliers. We believe the total population excluded from our initial estimate is far less than the tens of thousands asserted by the passenger vessel industry association.

One commenter stated that the 204,835 mariners that TSA and the Coast Guard estimated would be impacted by the rule in the RIA accounts for credentialed mariners, but omits non-credentialed mariners.

We agree that the approximately 205,000 mariners estimated in the RIA only accounts for credentialed mariners. However, we believe the other mariners that are not required to carry a mariner credential under the existing Coast Guard regulations were included in other areas of our population estimate. For example, in our research on the affected population, we accounted for workers in such categories as vessel operations and port support; barge operators; and offshore liquid bulk. Although we did not specifically calculate the number of mariners without existing credentials, we nevertheless believe they were captured in our population estimate. The comments that we received from industry contained no specific information on this matter, and therefore, we did not adjust our population estimate in response to this comment.

The Owner Operator Independent Drivers Association (OOIDA) asserted that between 500,000 and 1,000,000 truckers access the ports, regularly or occasionally. The association asserted that this population was underestimated in the RIA.

TSA and the Coast Guard value the concern expressed by the trucking trade association about our estimate for the number of commercial truck drivers accessing facilities regulated by 33 CFR subchapter H. While estimating the number of port truckers in the NPRM,

TSA and Coast Guard contacted many subject matter experts and analyzed numerous sources of public data. We found no consensus on the number of truckers regularly accessing facilities affected by this rule. We have, however, adjusted our initial NPRM estimate of affected commercial truck drivers.

After publication of the NPRM, it came to our attention that we may have excluded some foreign commercial truck drivers who operate out of Canada and Mexico. In order to correct this oversight, we have increased our total population estimate by 20,000—to 770,000 from 750,000 to account for this segment of the trucking industry.

Although this upward adjustment to our population estimate may address some of the concerns raised above, TSA and the Coast Guard can find no data to support the claim made by OOIDA that there are between 500,000 and 1,000,000 commercial truck drivers accessing regulated facilities on a regular basis. We note that the facilities covered by this rule represent a fraction of the total maritime facilities operating in the United States, and that the organization provided no specific information about the source of its data used to support its assertion. For these reasons, we have not modified our population estimate beyond the final estimate of 770,000.

(b). Estimates of Employee Turnover for Population Are Too Low

Several commenters stated that the assumed employee turnover rate of 12 percent in the RIA for the NPRM was too low. The extreme employee turnover rates in various segments of the maritime industry, they noted, would make total compliance costs significantly higher than those estimated by TSA and the Coast Guard. Table 5 displays estimates of turnover rates provided by various commenters.

TABLE 5.—TURNOVER RATE ESTIMATES BY COMMENTERS

Industry	Turnover estimate (percent)
Passenger Vessel	70
	100
	200
	50–150
	60
	100
	50–75
	70–100
	>150
	100
	200
Inland Waterways	>50
	30–40
	20–135
Casino	20–40
	28
Trucking	130

TSA and the Coast Guard understand that many firms operating in the maritime industry experience a high level of employee turnover on an annual basis. We concur with many commenters that this is especially true for trucking firms and enterprises that rely heavily on seasonal labor (particularly passenger vessel operators conducting business on the inland waterways).

In attempting to estimate the number of enrollments over the 10-year period of analysis, we focused on utilizing an industry-level estimate for employee turnover, not a firm-level estimate. Namely, we were interested in the rate at which individuals enter and exit the affected industry or industries—not the rate at which they enter and exit unique firms or establishments. This is because an individual who moves from one covered employer in the maritime industry to another covered employer would not need a new TWIC, although such a labor shift would be counted in firm-level turnover estimates. Had we used a firm-level estimate, such as those provided above, we would have overestimated the number of enrollments; we would have, in essence, double counted. We did not receive any comments on industry-level employee turnover rates and, therefore, have not adjusted our estimate of 12 percent in the RIA.

5. Other Economic Comments

One commenter stated that there is a concern about TSA's ability to process applications under the TWIC rulemaking. The commenter was concerned that the number of applications may be far more than TSA and Coast Guard estimates, that system overloads may cause long delays before tight deadlines, and that the possibility for administrative mistakes is enormous.

TSA and the Coast Guard will do everything within their authority to ensure that there are sufficient resources to process all applications submitted to TSA under this rule. Furthermore, procedural safeguards, including new redress processes, will minimize the number of administrative oversights.

Comments submitted by the SBA Office of Advocacy stated that the rule may deter community residents from participating in local security committees, such as the AMS Committees maintained under 33 CFR subchapter H. In many instances, the SBA Office of Advocacy noted, local community residents often provide the greatest protection against security threats because they are most familiar with operations on the ground, and can easily detect anomalies that would indicate a security threat. By deterring these individuals from participating on AMS Committees, the SBA Office of Advocacy questioned whether the rule would do more harm to security than good.

The purpose of this final rule is certainly not to deter individuals from participating in the AMS Committees (other local security organizations would not be subject to the final rule). We recognize the value of these organizations in securing critical U.S. maritime assets, and we agree that, in many instances, local residents are often best qualified to identify suspicious activities and threats. Nevertheless, we also firmly believe that individuals who are members of such organizations should be vetted using security threat assessments in order to ensure that they do not pose a security threat to vital areas of the U.S. maritime transportation sector.

In order to counteract this potential deterrent effect, we changed the requirements in the final rule to ease the burden on AMS Committee members and participants of other local security organizations. The final rule states that AMS Committee members must do one of the following: Receive a name-based threat assessment from TSA, obtain a TWIC, or have passed a comparable security threat assessment, as determined by the FMSC (who is also the Captain of the Port).

6. Impacts to International Trade

Some commenters stated that the rule would have a negative impact on international trade, and that this cost was not accounted for in the RIA.

TSA and the Coast Guard understand that some isolated international markets may be impacted by the final rule. In light of comments received on the public docket, TSA and the Coast Guard acknowledge that the rule could have an impact on international trade. By raising the operating expenses of some firms that engage in international business, the rule could potentially increase the price of goods and services, thereby affecting the flow of commercial transactions across international

borders. However, we think this is unlikely given the amount of competition in many international markets. Furthermore, the prices of goods and services are determined by many factors other than firms' operating costs. We have no information or data that would allow us to estimate this potential effect, and commenters did not provide any specific information with respect to this impact.

7. Comments on the Initial Regulatory Flexibility Analysis

In order to evaluate potential impacts to small entities, as defined by the Regulatory Flexibility Act (RFA) and the SBA Office of Advocacy, TSA and the Coast Guard published an Initial Regulatory Flexibility Analysis (IRFA) in May 2006 in support of the TWIC in the Maritime Sector NPRM. We received several public comments that addressed many facets of the IRFA. As part of this final rulemaking effort, we have summarized and responded to all substantive comments.

(a). The Rule Imposes a Significant Burden on Small Entities and Does Not Meet the Requirements of the Regulatory Flexibility Act

Many commenters, including Advocacy, claimed that the rule imposes a significant burden on small entities as defined by the RFA and that the agencies did not complete an accurate analysis of the impacts of the rule on small entities. Other commenters said that small entities, especially vessels, do not need the level of equipment proposed in the rule for security.

In the IRFA published with the NPRM, TSA and the Coast Guard did not make a determination about whether the NPRM would have a significant economic impact on a substantial number of small entities, and asked for comments on the issue. As demonstrated above, many commenters believe the rule would have a significant economic effect on many small businesses. In making a determination for this final rule, we agree with these comments, and have concluded that the rule will have a significant economic impact on a substantial number of small entities.

However, in drafting the final rule we have made significant changes that we believe will decrease adverse impacts on small businesses. TSA and the Coast Guard do not believe the rule will force small entities to leave the various markets in which they conduct business. In fact, TSA and the Coast Guard made a number of material changes to the original proposal in order to specifically address concerns about its impact on small entities.

First, and perhaps most importantly, small vessels and facilities will no longer need to purchase biometric smart card readers or other equipment in order to comply with the rule. Instead, the Coast Guard will conduct spot checks of credentials with handheld smart card readers. We believe this change will significantly reduce the economic burden on small entities. (As stated elsewhere in this document, however, TSA and the Coast Guard will initiate a future rulemaking that would require the use of such equipment. When this happens, we will reevaluate all costs estimates and impacts to small entities.)

Second, TSA and the Coast Guard have eliminated the recordkeeping provisions from the final rule. This modification should also reduce the burden on small entities.

Third, we have added to the final rule provisions to accommodate newly hired employees at businesses affected by the rule. These employees, after having applied for a TWIC, will be allowed limited access to secure areas for 30 consecutive days, subject to certain restrictions. This 30 day period may be extended an additional 30 days by the cognizant Coast Guard COTP if TSA does not act upon the individual's TWIC application within the original 30 days.

Fourth, we have added to the final rule provisions for employee access areas on passenger vessels and ferries. These areas are defined as spaces within the area over which an owner or operator has implemented security measures for access control. Employee access areas are open only to employees and not passengers; they are not secure areas and therefore do not require a TWIC for unescorted access. As stated above, this should further reduce the burden on some small businesses, especially passenger vessels reliant upon seasonal employment.

Finally, TSA and the Coast Guard will allow certain facilities to submit amendments to their security plans in order to redefine their secure areas. We included this provision in the final rule to give these facilities the opportunity to more closely align and perhaps narrowly focus their secure areas on those areas that are directly related to maritime transportation or most at risk of a transportation security incident. The provision may result in a smaller secure area, which would reduce the number of employees and visitors who may need a TWIC for unescorted access.

Many of these new provisions are designed to help small entities comply with the rule in a cost efficient manner, without sacrificing the security goals of the rule.

The International Association of Drilling Contractors (IADC) asserted that there are many unfounded assumptions regarding the economic impact of the NPRM involving the number of persons that need a TWIC, the rate of personnel turnover, the costs associated with procurement and installation of required equipment, and the recurring costs of maintaining the TWIC and associated equipment. The IADC went on to state that many qualifying small entities provide valuable services. Other commenters voiced similar concerns.

TSA and the Coast Guard acknowledge that there are a number of assumptions in the RIA that we published with the NPRM. Where appropriate, we have modified some of the assumptions in the RIA for the final rule based on input from industry.

Many of the cost estimates and assumptions that generated the most comments (e.g., costs associated with technology requirements and recordkeeping costs) are no longer germane to this rulemaking because of modifications to the final rule. For example, TSA and the Coast Guard will no longer require affected entities to purchase biometric smart card readers or keep records of individuals who access secure areas. While these provisions may be required in a future rulemaking, we will revisit the associated cost estimates at that time. As for the assumed turnover rate, we have addressed that above.

TSA and the Coast Guard disagree with IADC's suggestion that this rulemaking fails to meet the requirements of the RFA. To the best of our ability, we identified the firms affected by the rule, the economic impact to those firms, and the regulatory alternatives contemplated during the rulemaking process. Furthermore, we believe that the final rule includes significant alternatives to the original proposal that should decrease the impact to small entities. We therefore believe that this final rule meets both the letter and the spirit of the RFA.

The SBA Office of Advocacy, expressing concerns raised by several small businesses, asserted that the IRFA for the NPRM failed to include many small businesses in the maritime towing (*e.g.*, tugboats, towboats, and barges) and passenger vessel industries (*e.g.*, ferries; sightseeing, excursion, and dinner boats; gaming vessels; whale watching boats; and eco-tour vessels). The SBA Office of Advocacy also stated that the economic analysis and IRFA failed to include other affected sectors. In its comment, the SBA Office of

Advocacy noted that a charter bus operator picking up cruise ship passengers at a port terminal would need a TWIC (or a credentialed escort) if he or she accessed a secure area. Advocacy recommended that TSA and the Coast Guard re-assess whether the economic analysis and IRFA encompass all regulated sectors.

In light of the comments above, we reviewed the industries identified in the IRFA as being affected by the rule. Many of the small businesses in the maritime towing and passenger vessel industries fall under the North American Industrial Classification System (NAICS) codes 488330 Navigational Services to Shipping; 336611 Ship Building & Repairing; 532411 Commercial Air, Rail, & Water Transportation Equipment Rental and Leasing; 483114 Coastal and Great Lakes Passenger Transportation; and, 48721 Scenic and Sightseeing Transportation, Water. These industries were included in the IRFA that we published along with the NPRM. However, we did not include Gaming Vessels in the IRFA and they will most likely be affected by the final rule.

Based on the comments above, we have included two additional NAICS codes in the FRFA—gaming vessels fall under 713290 Other Gambling Industries and 713210 Casinos (except Casino Hotels).

With respect to the charter bus example cited by Advocacy, TSA and the Coast Guard recognize that some small businesses outside the maritime transportation sector that were not identified in the IRFA may be affected by the final rule. The example given by Advocacy in its comment is plausible—TSA and the Coast Guard do not dispute that charter bus operators may access cruise ship terminals.

For the most part, however, we do not believe that cruise ship terminals and other large facility owners/operators currently allow charter bus operators and other independent firms or visitors to freely move about secure areas without supervision or monitoring. Many of these large facilities where cruise ships dock have reams of valuable cargo on their property and consequently have an economic incentive to monitor visitors, including bus operators. Therefore, we believe that many facilities will choose to use a credentialed escort in many of these instances. For these reasons, we believe the FRFA now identifies the industries that will be affected by this rulemaking.

The American Sail Training Association (ASTA) asserted that the IRFA and NPRM do not appear to take into account vessels such as the tall ships owned by ASTA members because the regulatory analysis focuses on the small businesses included within the subchapter H vessels, facilities and outer continental shelf facilities. ASTA members are not within that category.

Only vessels, facilities and OCS facilities regulated by 33 CFR subchapter H will be required to comply with the requirements of the final rule and incur associated costs. For this reason, we did not consider impacts to vessels not regulated by 33 CFR subchapter H.

(b). The Rule Fails To Meet the Maritime Transportation Security Act

In support of concerns raised by small business representatives, the SBA Office of Advocacy commented that the limited maritime TWIC being proposed exceeds TSA and Coast Guard's statutory mandate. Specifically, Advocacy asserted that MTSA did not require the complex and costly design or the potentially expensive smart card readers that TSA and the Coast Guard proposed in the NRPM. Advocacy also noted that many small businesses felt that there should be a single credential and security threat assessment for the entire transportation sector.

Section 102 of MTSA requires the Secretary of DHS to issue a biometric transportation security card to individuals with unescorted access to secure areas of vessels, facilities, and OCS facilities. MTSA did not specify what type of biometric card the Secretary should issue. We believe the TWIC, which can accommodate many kinds of biometrics, privacy protections, and security mechanisms, meets the letter and spirit of the law.

Also, as previously stated, this final rule will not require vessels, facilities, or OCS facilities to purchase biometric smart card readers. TSA and the Coast Guard will address the technology and card reader issues in the future. We will address comments relating to these issues in the future.

(c). Whether the Rule Meets Previously Stated Goals

Commenters, including the SBA Office of Advocacy, stated that the NPRM fails to meet the objectives of the TWIC concept as originally envisioned, that is, a single biometric card and a single background check for the entire transportation sector. Commenters argued that duplicative credentials and clearances that may include separate state and local requirements may continue to be required because TWIC is limited to the maritime sector. Also, the commenters stated that the original intent of the TWIC was to help ease access to secure areas, not to require a TWIC to enter them.

TWIC is a biometric transportation security card, mandated by sec. 102 of MTSA, which TSA and the Coast Guard are introducing for use in secure areas of the maritime transportation sector. As stated in the preamble to the NPRM, DHS is currently exploring introducing the TWIC into other modes of the transportation sector. In the NPRM, we solicited and received comments on this issue.

With respect to this final rule, the purpose of TWIC is not to facilitate access to secure areas of the national transportation sector, as some individuals asserted in their comments. While attempting to preserve owner/operator's ability to exert control over their secure areas, this final rule adds an additional level of security to these critical areas of the nation's maritime assets through the use of TWIC. The primary objective of TWIC has been, and will be, to increase security without unnecessarily compromising the flow of goods and services in the economy.

Comprehensive security threat assessments are a vital part of this objective. Some commenters expressed concern that the rule would create duplicative threat assessments and credentials. TSA and the Coast Guard have made every effort in this final rule to avoid creating requirements that would cause individuals to obtain redundant security threat assessments. For example, individuals who have recently completed a security threat assessment for an HME, the FAST Program, or one of the Coast Guard's mariner credentialing programs, will not undergo a new TSA security threat assessment as a result of the TWIC rule. TSA will also review other government background checks in order to determine if they are comparable to those being conducted under the authority of this rule. Furthermore, if DHS decides to require TWIC in other modes of the transportation sector, we will make every effort to avoid duplicative or inconsistent security threat assessment standards.

As stated above, several commenters asserted that the rule would require duplicative credentials for some individuals. For example, one commenter suggested that a commercial truck driver who picks up a package at an airport and delivers it to a port terminal may have to hold two credentials under the provisions of the rule. TSA and Coast Guard agree that this scenario is plausible. Some individuals, due to different circumstances, may have to carry multiple credentials. Unfortunately, we

cannot guarantee that individuals affected by the rule will have to carry only one credential. Neither TSA nor the Coast Guard has the legal authority to prevent private companies from issuing their own, proprietary identification credentials. However, TSA and the Coast Guard believe that many private firms currently issuing their own identification credentials may cease to do so after TWIC is introduced, because it may result in a cost-effective solution to existing credentialing systems.

(d). The Rule's Effect on Current Labor Shortage Affecting Small Entities

Several commenters made general remarks about how the TWIC rule will make labor shortage issues worse for small entities. Industry associations, small firms, Advocacy, and individuals all opined that the user fees proposed in the NPRM; the ''wait time'' to obtain a security threat assessment and a credential; and the inconvenience associated with traveling to an enrollment center would all negatively impact the work force utilized by small entities.

TSA and the Coast Guard understand that some areas of the maritime transportation sector are experiencing labor shortages. As noted previously, however, we believe that the shortage of labor in many areas of the maritime industry is a function of factors outside the control of either TSA or the Coast Guard.

Nevertheless, the final rule may have an impact on some labor markets. TSA and Coast Guard concur that some individuals—due to the user fees, security threat assessment policies, or other factors—may no longer seek employment at businesses regulated by 33 CFR subchapter H as a result of this rule. To the extent possible, though, we have drafted the final rule so that it would not adversely affect the already limited supply of labor in certain segments of the maritime transportation sector. We needed to balance this effort, of course, with the primary security objectives of the rule. We believe the following amendments to the final rule will help ease the potential adverse impacts of the rule on the labor supply while achieving the security goals of the rule:

- Provisions to accommodate new hires and persons who have reported their TWIC as lost, damaged, or stolen.
- An allowance for certain facilities to amend their Facility Security Plans (FSPs) to redefine their secure areas, and new definitions for passenger access areas and employee access areas.
- Expanded response time for applicants to appeal an adverse determination, correct an open criminal disposition, or apply for a waiver from 30 or 45 days to 60 days.
- Expanded group of applicants eligible to apply for a waiver after being disqualified because of mental incapacity.
- Expanded the group of non-U.S. nationals who meet the immigration standards to include foreign nationals who are students at the U.S. Merchant Marine Academy or comparable State college; commercial drivers licensed in Canada or Mexico transporting hazardous materials into and within the U.S.; citizens of Canada or Mexico who conduct business in the United States under a NAFTA visa; and a variety of professionals and specialists who work in the U.S. maritime industry on restricted visas.
- Provisions for employee access areas on passenger vessels and ferries.

Some commenters specifically mentioned that being forced to pay the enrollment costs for their employees will be harmful to them. Laying out the same argument as other, larger firms, many small business owners who submitted comments to the docket pointed out that they would not be able to pass application costs onto college students, low wage earners, or other employees that typically work for small businesses.

We note that this is not a requirement of the rule, but we agree that in some markets, owners/operators may pay the TWIC user fees for their employees. This may be especially true for employers that operate in sectors with tight labor markets. In other industries, however, this will probably not be true. For instance, in highly unionized workforces where wages are high and benefits are generous, employers will most likely not be forced to pay TWIC user fees. Due to this high level of uncertainty, we did not quantify this potential burden to employers in the RIA.

Others said that seasonal employees are not able to afford the application fees or the cost of traveling to an enrollment center.

TSA is required by law to recover fees for the costs it incurs to provide all program services. Therefore, the agency cannot make any concessions with respect to the user fee, even for seasonal employees. TSA and the Coast Guard have included some provisions in the final rule that may reduce the burden on seasonal employees. These provisions, such as employee access areas, are detailed above.

Another commenter said that the ''waiting period'' for a TWIC is a hardship for small entities because they will have additional costs involved with interviewing new employees.

As stated earlier, the final rule contains a provision that will allow new employees to have limited access to secure areas for 30 consecutive days, subject to other restrictions detailed in the regulatory text. In addition, this may be extended an additional 30 days by the cognizant Coast Guard COTP if TSA does not act upon the individual's TWIC application within the original 30 days. This provision should ease the burden on small entities.

Some commenters discussed how the burdens employees face in obtaining TWICs are harmful to small entities. Some, for example, said that small companies are competing with larger companies for workers, and larger companies are more competitive because they are more capable of absorbing TWIC enrollment costs. Some commenters said that they will not be able to fill seasonal and short-term positions due to the TWIC requirements. One commenter said that small entities subject to TWIC will not be able to compete with other small service entities that are not subject to TWIC requirements. Another said that they will not be able to compete for labor with other service industries.

One commenter said that the burdens of TWIC on employees will result in further wage increases to retain employees in their industry. Others said that the costs and burdens of TWIC will force employers to go to other industries, which is a hardship for small entities.

TSA and the Coast Guard realize that small businesses face unique challenges in complying with the final rule. We recognize that the rule may impact employees as well as other facets of small entities' businesses. During the rulemaking process, we analyzed several alternatives that would have lessened the impact to small entities.

For example, we examined the possibility of exempting the employees working for small businesses from the requirements of the final rule. Furthermore, we also analyzed the possibility of exempting industries with a high proportion of small businesses (*e.g.*, passenger vessel industry) from the provisions of the rule. Both alternatives were deemed incompatible with the security objective of the rulemaking since 33 CFR subchapter H specifically applies to vessels, facilities, and OCS facilities that have been identified by the Coast Guard as presenting a risk for a transportation security incident.

Moreover, statutory constraints also prohibited us from further considering this option.

TSA and Coast Guard did, however, include a number of new provisions to help small businesses comply with the rule. These provisions, such as the new hire provision, passenger and employee access areas and allowances to certain facilities to redefine secure areas, are detailed elsewhere in this section.

Many commenters, including the SBA Office of Advocacy, expressed concern that businesses utilizing seasonal or temporary workers could be significantly impacted by the rule. For example, small tour boats and sightseeing vessels frequently hire high school and college students to work on the boats during the summer. However, because these employees could be required to obtain a maritime TWIC before they could begin work, the proposed rule could impose significant costs and time burdens on these small businesses.

We realize that seasonal and temporary workers are a vital supply of labor for many passenger vessels and other small businesses regulated by this final rule. We also understand that the requirement to obtain a TWIC may represent a financial burden for some seasonal employees, especially high school and college students who may only work during the summer months. In writing this rule, we looked at several alternatives that would minimize this burden without compromising security.

First, we considered exempting small passenger vessels and other regulated entities utilizing seasonal laborers from the requirements of the rule. This would clearly eliminate any concerns about labor shortages or financial burdens that many small businesses expressed during the comment period for the NPRM. We determined after careful analysis, however, that this alternative would not meet the security objectives that are the rationale for the rule, as passenger vessels subject to the security assessment and plan requirements in 33 CFR part 104 are at high risk for a transportation security incident due to the number of people they transport, which makes them an attractive target for terrorists. TSA's and the Coast Guard's statutory obligations also prevented us from adopting this option.

Second, we investigated the possibility of allowing owners/operators to grant individuals who have applied for a TWIC limited access to secure areas for 30 days. As stated elsewhere, we have included this provision in the final rule, which we hope will reduce the regulatory burden for small entities.

Finally, in another effort to minimize the burden on small vessels, we created employee access areas in this final rule. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the vessel security plan. We believe that this new provision should reduce the regulatory burden on many small passenger vessels, especially those that primarily utilize and rely on seasonal labor.

(e). Costs of the Escorting Requirement

Another commenter mentioned that the escorting burden is particularly difficult for small entities since they usually do not have excess crews or manpower to meet these requirements.

We agree that for some small entities the requirement to provide escorts for visitors and others may prove to be a substantial burden. TSA and Coast Guard also do not dispute commenters' claims that many small entities may not have excess employees to handle this provision. We feel, however, that many commenters interpreted the definition of escort to require the physical presence of one escort for each individual without a TWIC at all times while in a secure area. TSA and Coast Guard did not intend this provision to be interpreted in this manner.

Instead, we expect that when in an area defined as a restricted area in a vessel or facility security plan, escorting will mean a live, physical escort. The specifics of each vessel or facility will determine the scope of the escort required. Outside of restricted areas, however, such physical escorting is not necessary, so long as the method of surveillance or monitoring used is adequate to allow for a rapid response should an individual ''under escort'' be observed in an area where he or she has not been authorized to go or is engaging in activities other than those for which access was granted. We believe that this interpretation may significantly decrease the burden of this provision for small entities.

Moreover, in the final rule, TSA and the Coast Guard have taken steps that may further reduce this burden for small businesses. For example, the final rule contains a provision for passenger vessels and ferries to establish employee access areas, which may decrease the need for certain small entities to supply some employee with escorted access to secure areas.

The final rule also contains a provision that allows certain facilities to redefine their secure areas by submitting an amendment to their security plans to the Coast Guard. TSA and the Coast Guard believe that this new allowance may help some small entities limit the burden of providing escorted access to some employees and visitors.

Although TSA and Coast Guard contemplated easing this requirement of the rule for small entities, we ultimately determined that we could not do this without comprising security.

The SBA Office of Advocacy and other commenters noted that it is likely that many businesses will seek to avoid the maritime TWIC requirements by providing (or requiring) the use of dedicated, credentialed escorts as an alternative. Some commenters recommended that TSA and the Coast Guard consider the likelihood that this will occur and whether it changes the cost projections for the proposed rule.

Although we realize that affected entities may comply with the rule in this manner, TSA and the Coast Guard have no information that would allow us to calculate the probability of this occurrence, making it difficult for us to adjust our cost projections. Credentialed escorts are specifically recognized as an acceptable means of complying with the final rule. Each business will evaluate the most cost effective way to comply with the rule, given its operational situation. TSA and the Coast Guard included the escort provision in the rule to potentially reduce the economic burden of the rule, provide flexibility, and maintain security.

(f). Required Equipment Is Too Expensive for Small Companies

Many small entities expressed concern about the cost of equipment. Several small vessels were concerned about how well equipment would work on vessels.

The final rule will not require vessels, facilities, and OCS facilities to purchase and maintain new equipment. TSA and the Coast Guard will address this issue in the future and will revisit all cost estimates and equipments requirements at that time.

E. Comments Beyond the Scope of the Rule

We received many comments concerning issues that are outside the scope of the NPRM. Many suggested port security grants be used to pay for TWICs and TWIC implementation, while others suggested that funding for implementation be made available in the federal budget. One commenter specifically requested a 90/10 matching of federal grant monies be appropriated to offset logistics costs. While these

comments are outside of the scope of the rule, we would like to note that the DHS port security grant program has already been revised to include applications for costs associated with implementing TWIC.

IV. Advisory Committee Recommendations and Responses

We received recommendations from three DHS advisory committees: The National Maritime Security Advisory Committee (NMSAC), the Merchant Personnel Advisory Committee (MERPAC), and the Towing Safety Advisory Committee (TSAC). Each committee reiterated some of the comments that have already been addressed, above, in the ''Discussion of comments and changes'' section. We have not repeated those concerns or comments in this section. Rather, we limit this discussion to those comments or recommendations that are not reflected elsewhere in this final rule.

A. National Maritime Security Advisory Committee (NMSAC)

NMSAC recommended that the final TWIC regulations indicate that if an individual who regularly works in a secure area has not obtained a TWIC, has been denied a TWIC, or has had his or her TWIC revoked, that person cannot have access to secured areas.

We do not agree with this recommendation, as the TWIC requirement only applies to individuals seeking unescorted access to secure areas. An individual who does not have his TWIC, either because he has not obtained one, been denied one, or had it revoked, could still be provided escorted access. Nothing in the final rule, however, requires that the owner or operator of a facility or vessel provide escorted access.

B. Merchant Personnel Advisory Committee (MERPAC)

MERPAC recommended that the Coast Guard delay the implementation of the MMC, separating the implementation of the MMC from the TWIC implementation, until the TWIC program is deemed successful.

This recommendation is more properly addressed in the Coast Guard's Supplemental Notice of Proposed Rulemaking (SNPRM) titled ''Consolidation of Merchant Mariner Qualification Credentials,'' found elsewhere in today's issue of the **Federal Register**. We note, however, that instead of issuing a final rule to implement the MMC, the Coast Guard has instead published an SNPRM, thus accepting at least part of the recommendation to delay MMC implementation.

The committee recommended that Coast Guard and TSA find other funding sources for the TWIC. They further asked that, if this recommendation be rejected, TWIC applicants be required to only pay the actual production costs of the cards, not the administrative costs of TSA.

Congress mandated that TSA fund the TWIC program out of user fees (see sec. 520 of the 2004 DHS Appropriations Act), thus, we are unable to consider this recommendation at this time.

MERPAC recommended that the next round of Port Security Grants be made available to every mariner, transportation worker and owner/operator to pay for this unfunded mandate. We appreciate this comment; however, the Port Security Grant Program is not part of this rulemaking.

MERPAC asked, ''Who will determine how much is the correct amount of profit for this contractor to make off of the American Citizens that will require this identification?'' They added that this program, from information collection to card activation, must be conducted by the U.S. government, not contractor. They requested that ''If there is a stated percentage of profit that is appropriate, that percentage should be included in the rulemaking for comment. When the bi-annual review is published, the percentage of profit should again be broken out, particularly before any increase in fees is approved.''

Nothing in MTSA or the other laws and regulations authorizing the TWIC program prohibits the United States Government from contracting for appropriate commercial services in support of the program. In fact, it is the policy of the United States Government to rely on the private sector for needed commercial services, where appropriate. TSA is, however, committed to reducing the cost of this program to individuals required to obtain the card to the extent possible. To that end, TSA is developing a competitive solicitation for the services. There has been a significant amount of interest on the part of the private sector in this solicitation. Among the evaluation criteria is the reasonableness of the cost as compared to the government's independent cost estimate. In addition, the contracting officer is responsible for ensuring that all contractor costs are fair and reasonable. There is no stated percentage of profit that is appropriate, and therefore we cannot include that percentage in the rulemaking for comment. Instead, we are looking at the overall cost to the public and will use private innovation and competitive process to obtain the best possible overall cost for the public.

MERPAC recommended that TSA facilitate the payment of any fees via the pre-enrollment web site, and that TSA begin the vetting process with information submitted at this Web site. They went on to request that mariners be able to pay the fees required by credit card or cash, and not just money order, check, or wire transfer.

During the initial rollout of the TWIC program, applicants must pay the fee for the credential at the enrollment center, rather than on-line. We may develop processes in the future to accommodate payment during pre-enrollment, but we cannot do so at this point. We will accept credit cards, cashiers checks, or money orders. Accepting cash or personal checks create opportunities for fraud that we wish to avoid.

The committee questioned some language from the NPRM, asking ''[o]n pg 29403, section (e): This section states 'After the individual has been granted access to the facility, the owner/operator may opt to notify the TSA system that access privileges have been granted to this worker at that facility.' MERPAC would like an explanation of this section, as it seems unnecessary.''

The cited language refers to the process known as privilege granting. Under that process, as proposed in the NPRM, one way for a facility or vessel to meet their requirement to validate TWICs (*i.e.*, ensure that they have not been invalidated by TSA) was to tell TSA those individuals to whom they were granting access. This information would be stored in the TSA TWIC database. Then, as cards were invalidated for any reason, the database would ''push'' that information to those facilities or vessels listed as having granted access privileges to that card. The process necessarily involves a centralized access control system at the facility or vessel, and as such would not work as a solution for everyone.

MERPAC asked TSA to explain the two year redesign, mentioned on page 29429 of the NPRM, by explaining what is involved, and explaining why the card holders should pay for said redesign.

The technology for the credential will be improved to add the contactless application and other security features as they become available. These improvements are standard items in complex programs, and as spread across the affected population over time, have a minimal impact on cost.

MERPAC recommended that the rule require TSA to complete each security threat assessment and issue a TWIC within 96 hours from enrollment. They

also recommended that TSA outline the procedures for notification to the applicant when a timely processing cannot be accomplished.

As discussed above, in the section entitled ''Adjudication Time,'' it is not feasible to complete a full threat assessment, including the collection of all of the information required to do so and issue a biometric credential within 96 hours. First, it is important to state that the TWIC program does not have a mandatory ''waiting period.'' Rather, we must adjudicate the security threat assessment of each applicant following enrollment and each case naturally entails processing time. During the initial enrollment rollout, owners/operators must give ample notice to workers so that the threat assessment can be completed before the workers are required to present a TWIC to gain access to secure areas. Our goal is to process security threat assessments and manufacture TWICs within 30 days, and our experience with other programs indicates that this is quite possible. However, processing time may increase for an applicant with a criminal history or other disqualifying information, and when an appeal and/or waiver is required.

The time period needed to complete security threat assessments during the TWIC prototype is not a good model from which to make comparisons. TSA was not able to complete a CHRC during Prototype, because there was not a regulation in place requiring a fingerprint-based check. Therefore, the time needed to complete the threat assessment was much shorter than is typical. However, the Prototype provided data on enrollment and card production processing times. We will process applications as they are received. After applications are received and sent for security threat assessment, individual processing times will vary based on the complexity of the adjudication.

In response to the many comments on adjudication time, TSA is amending the information required for enrollment to help expedite the adjudication process. Most of the new information is voluntary; however, providing it should help TSA complete adjudications more quickly. All of the amendments apply to HME and TWIC applicants. First, applicants who are U.S. citizens born abroad may provide their passport number and CRBA. These documents expedite the adjudication process for applicants who are U.S. citizens born abroad. In addition, applicants who have previously completed a TSA threat assessment should provide the date and program for which it was completed. Applicants should state if they hold a federal security clearance, and if so, the date and agency for which the clearance was performed.

A general review of background checks and security threat assessments across government and in the private sector will show that the processing time for a TWIC or HME is far below the average time to complete an assessment. In any event, as described above in the discussion of the Coast Guard's provisions, we have included provisions in the final rule to provide relief to the owner/operator who needs to provide a new hire with unescorted access to secure areas before the individual's TWIC has been issued.

MERPAC recommended that those persons that need access to vessels subject to MTSA that provide counsel and religious guidance to seafarers should be required to obtain a TWIC, but be exempted from the fees.

We disagree with this recommendation. As already stated, Congress has mandated that all costs of the TWIC program be funded through user fees. Thus, eliminating the fees for one portion of the affected population automatically increases the fee for the remaining population. We do, however, recognize the importance of allowing these individuals access to the mariners they serve. These individuals may be escorted into secure areas if they choose not to obtain TWICs.

MERPAC requested that TSA describe the process for card renewal.

Renewal applications will go through the same process as initial applications: applicants will need to enroll, provide fingerprints, have a new security threat assessment completed, and return to the enrollment center to activate their TWIC.

MERPAC recommended that an additional section be included in the rulemaking, addressing the obligations and training requirements that should be necessary for the employees and managers of the enrollment centers, those employees activating and issuing TWIC cards, and any other employees associated with this program.

We do not agree with this comment. Procedures and standards for the contractor providing enrollment services will be part of the contract between TSA and the contractor. They do not impose obligations on the general public, and as such are not appropriate for inclusion in the regulations. We can assure the committee, however, that these topics will be covered.

MERPAC recommended the TWIC application itself be revised stating, ''Item 10 of [proposed 49 CFR] 1572.17 requires a job description and listing of a primary facility where the card holder anticipates using the card. This information should be removed from the application, so that mariners are not accused again of submitting incomplete applications. The purpose of the collection of this information could be accomplished by changing the attestation on page 29456, which should state that the applicant attests that they have a legitimate need for the card, that they understand its uses and obligations. They should not be asked to attest that the card 'as part of my employment duties' as for an applicant, that may not yet be true.''

The purpose of having the applicant list the job description and primary facility, if known, is to ensure that employers whose employees do not need TWICs do not send their employees to enrollment centers just to get a full background check on them. This information, however, is not required if the applicant does not yet have a job description or primary facility. As such, a blank entry on the application will not prevent it from being processed.

MERPAC noted that we address the need to have employers and their employees notify TSA of a security violation by a person attempting to access a facility with a fraudulent or tampered card, and asked that we also define what the procedures and penalties are for a violation.

It is unclear whether the committee is asking about the penalties for a failure to notify, or if they are asking about the penalties for someone found with a fraudulent or tampered card. In the case of the former, the penalty is found in the general penalty provision of 33 CFR part 101. In the latter case, the penalties are found in 49 CFR part 1572.

MERPAC recommended that foreign riding gangs should be subject to the same requirements as U.S. mariners, and that they be subject to all the same requirements of U.S. mariners: background checks, drug testing, etc.

If foreign riding gangs are currently required to obtain a U.S. MMD, license, COR, or STCW endorsement, they would also be required to obtain an MMC. This regulation does not propose to change the population of people who must obtain a mariner credential. Foreign riding gangs must meet the same requirements for lawful status as any other TWIC applicant. Vessels operating in waters outside of the United States will not need to have TWIC implemented on board, therefore the TWIC provisions will not be applicable to riding gangs if the vessel they are working on is operating in non-U.S. waters.

MERPAC recommended that foreign truck drivers and foreign technicians be specifically addressed in the final rule, providing detailed procedures to accommodate their presence in facilities and on vessels.

We disagree. We have made changes to the final rule that, we believe, will allow foreign workers who are lawfully present in the United States and legitimately working at facilities or on vessels to get a TWIC if their work requires them to have unescorted access to secure areas. Those foreigners who still cannot get a TWIC will need to be escorted, as that term has been clarified elsewhere in this final rule.

MERPAC recommended that all TWIC holders be automatically enrolled in the Trusted Travelers Program, and that facial recognition software should be considered as a means of providing access with a TWIC.

To date, there is no domestic ''Trusted Travelers'' program, and implementing such a program is outside the scope of this rulemaking. The criteria for participants in TSA's ''Registered Traveler'' program are still being developed. We will keep this recommendation in mind for future consideration. Additionally, neither the NPRM nor this final rule prohibit the use of facial recognition software by facilities or vessels, so long as the software is able to integrate with all of the TWIC requirements found in this final rule.

D. Towing Safety Advisory Committee (TSAC)

TSAC requested an investigation on the impact TWIC will have on new/existing marine employees. The committee expressed concern about the costs to commerce, and noted that they believe the costs were undervalued and logic was not applied. They requested an economic analysis about the impact on commerce.

All of the issues raised in this request are addressed, in some form, in the Final Regulatory Assessment for this rule. This document is summarized below, but is also available on the docket at the locations listed in the **ADDRESSES** section above.

They also requested a formal ''task statement'' so they can work with Coast Guard and TSA in the next stage of the rulemaking. We appreciate this offer, and will keep it in mind as we begin developing our second rulemaking (regarding reader requirements).

V. Rulemaking Analyses and Notices

A. Executive Order 12866 (Regulatory Planning and Review)

This rule is a ''significant regulatory action'' under section 3(f) of Executive Order (E.O.) 12866, Regulatory Planning and Review and therefore has been reviewed by the Office of Management and Budget. E.O. 12866 requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. A Final Assessment is available in both the TSA and Coast Guard dockets where indicated under the ''Public Participation and Request for Comments'' section of this preamble. A summary of the Assessment follows.

Regulatory Impact Assessment Summary

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 (E.O. 12866) directs each Federal agency to propose or adopt a regulation only if the agency makes a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. § 2531–2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (Public Law 104–4) requires agencies to prepare a written assessment of the costs, benefits and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

In conducting these analyses, TSA and the Coast Guard have determined that this rule:

1. Is a ''significant regulatory action'' as defined in E.O. 12866.

2. Has a significant economic impact on a substantial number of small entities. We have provided a Final Regulatory Flexibility Analysis, which is available in the Regulatory Impact Assessment that is located on both public dockets.

3. Will not impose significant barriers to international trade.

4. Does not impose an unfunded mandate on State, local, or tribal governments, but does on the private sector as costs exceed the inflation adjusted $100 million threshold in at least one year.

The regulatory impact assessment (RIA) is a joint effort of TSA and the Coast Guard. The reader is cautioned that we did not attempt to replicate precisely the regulatory language in this summary of the RIA; the regulatory text, not the text of the RIA or this summary, is legally binding. A copy of the comprehensive RIA can be found on both public dockets.

Impact Summary

Section 102 of MTSA requires the Secretary of the Department of Homeland Security to issue a biometric transportation security card to individuals with unescorted access to secure areas of vessels and facilities. Under this authority, DHS has developed this final rule, and this summary provides a synopsis of the costs and benefits of the final rule.

Benefits of the Final Rule

The final rule will increase security at vessels, facilities, and OCS facilities regulated by 33 CFR chapter I, subchapter H. It will accomplish this by: (1) Reducing the number of high-risk individuals with unescorted access to secure areas of vessels, facilities, and OCS facilities through the use of robust security threat assessments, and (2) improving access control measures in the maritime transportation sector by permitting only those with biometric credentials to have unescorted access to secure areas of vessels and facilities.

Costs of the Final Rule

In estimating the economic cost of the final rule, we have made a number of adjustments to our original forecast published in the NPRM. First, as the final rule includes significant changes to the NPRM, we have accounted for those modifications in our estimates. For example, the final rule will not require vessel, facility, and OCS facility owners/operators to install and maintain smart card readers for access control purposes, keep access control records, or submit TWIC addenda to security plans. Compliance costs associated with these requirements therefore no longer appear in our estimates for the final rule; however, some of these costs are still reflected in the regulatory alternatives analyzed in the RIA.

Second, we have modified many of our cost estimates in response to comments received from individuals and firms in the maritime industry. Several commenters argued that we understated or failed to identify several costs associated with complying with the rule. In response to these comments, we have adjusted some of our estimates and assumptions. For instance, many

commenters asserted that we underestimated the opportunity cost to travel to TWIC enrollment centers. Based on several comments of this nature, we adjusted our estimate upward.

Third, we have better information with respect to many costs related to TSA's ability to deliver program services. This improved information is reflected in our new estimates.

After making these types of adjustments to our original estimate, we concluded that the 10-year cost of the rule, discounted at 7 percent, would range from $694.3 million to $3.2 billion. Much of the variance in our estimate is attributable to the uncertainty surrounding opportunity cost estimates and escorting cost estimates.

Table 6 displays the 10-year cost estimates for the NPRM and the final rule, discounted at 7 percent. The differences between the two estimates are also shown, with negative numbers appearing in parentheses. Figures showing 10-year cost estimates discounted at 3 percent and 0 percent are displayed in the comprehensive RIA, which is available on the public docket.

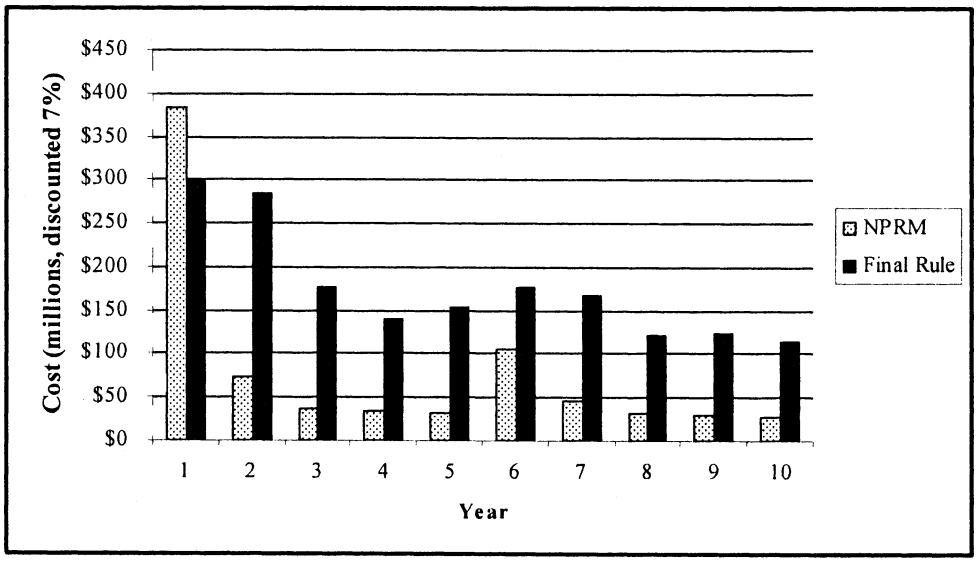
TABLE 6.—COST CHANGE, NPRM TO FINAL RULE

[$ millions, 7 percent discount rate]

Component	NPRM			Final Rule			Difference (Low–High)	Remarks
	Low	Primary	High	Low	Primary	High		
Enrollment Opportunity Costs.	.....	$71.8	.....	$73.8	$196.7	$393.5	$2–$321.7	Public comments on original time estimate and increased population.
Enrollment Service Costs.	.....	91.9	.....	.....	94.9	.....	3.0	Increased population.
Security Threat Assessment Costs.	.....	57.9	.....	.....	57.9	.....	0.0	Increased population but reduced technology costs.
TSA System Costs	.....	27.4	.....	.....	44.3	.....	16.9	Improved internal cost estimates.
Appeals and Waivers Opportunity Costs.	.....	5.7	.....	.....	5.9	.....	0.2	Increased population.
Card Production Cost	.....	29.5	.....	.....	31.9	.....	2.4	Improved internal cost estimates and increased functionality.
Issuance Opportunity Costs.	.....	89.0	.....	123.4	329.2	658.4	34.4–569.4	Public comments on original time estimate and increased population.
Program Office Support Costs.	.....	41.0	.....	.....	19.9	.....	(−21.1)	Improved internal cost estimates.
Compliance Costs, Facilities.	$299.0	312.1	$325.1	82.2	326.5	644.3	(−216.8)–319.2	Public comments on original estimates and changes to proposed requirements.
Compliance Costs, Vessels.	63.1	75.8	88.4	157.7	638.8	1,264.4	94.6–1,176	
Compliance Costs, OCS Facilities.	0.6	0.7	0.8	2.4	10.1	20.1	1.8–19.3	
Total	$777.0	$802.8	$828.6	$694.3	$1,756.3	$3,235.4	($−82.7)–$2,406.8	

As stated above, the primary cost estimates for the final rule differ from those estimated for the NPRM. While certain cost components, such as the card reader costs, were eliminated from the final rule, other adjustments, mainly to the enrollment opportunity cost and escorting cost estimates, caused a net increase in the total primary estimate. Table 7 displays the differences on an annual basis.

Table 7: Differences in Annual Primary Cost Estimates



B. Small Entities

Under the Regulatory Flexibility Act (RFA) (5 U.S.C. 601–612), we have considered whether this rule would have a significant economic impact on a substantial number of small entities. The term ''small entities'' includes small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. Individuals are not considered small entities for the purposes of the RFA.

In support of the NPRM, we conducted an Initial Regulatory Flexibility Analysis (IRFA) that did not conclude whether the proposed rule would have a significant economic impact on a substantial number of small entities. We solicited comments on the matter in order to become better informed on how the proposed rule would impact affected small entities.

After reviewing the public comments on the IRFA and the modifications to the final rule, we conducted a Final Regulatory Flexibility Analysis (FRFA), which is now available in the RIA on both public dockets. The public comments we received on the IRFA, which we summarized and responded to in the preamble to the final rule, addressed a broad array of issues specific to small entities, including the high cost of biometric smart card readers and other security infrastructure; the potential negative impact to businesses that predominantly utilize seasonal workforces; and the potential adverse effect on firms that must provide escorts for employees seeking access to secure and restricted areas, but do not possess unescorted access authority.

In completing the FRFA, we revised many of our initial cost estimates in response to both comments from industry and the changes to the rule that those comments produced. We have determined that the final rule will have a significant economic impact on a substantial number of small entities. In this summary, we provide a brief description of why our cost estimates have changed, and examples of how we have provided regulatory flexibility for small entities in an attempt to mitigate any adverse economic effects of the rule.

The primary reason for the determination that the rule will have a significant economic impact on small entities is that we have considerably revised our cost estimates for vessels and facilities to provide escorted access to employees and visitors in secure areas. During the public comment period, several individuals and firms expressed concern that we understated our original estimate for this requirement. In response to these comments, we increased our cost estimate for vessels and facilities to comply with this provision of the rule.

The final rule also contains several changes from the NPRM. For example, as stated elsewhere in this preamble, the rule no longer requires vessels, facilities, or OCS facilities to purchase, install, and maintain biometric smart card readers; it does not include the recordkeeping requirements proposed in the NPRM; and affected firms do not have to submit a TWIC addendum to the Coast Guard. These changes also caused us to adjust our cost estimates.

Table 8 displays how our low, primary, and high initial compliance cost estimates, as reported in the IRFA for the NPRM, have changed for small vessels. As previously described, these increased costs to small vessels are primarily a function of our increased cost estimate for small vessels to provide escorts to employees and visitors seeking access to secure and restricted areas.

Table 8: Difference in Initial Cost Estimates for Small Vessels

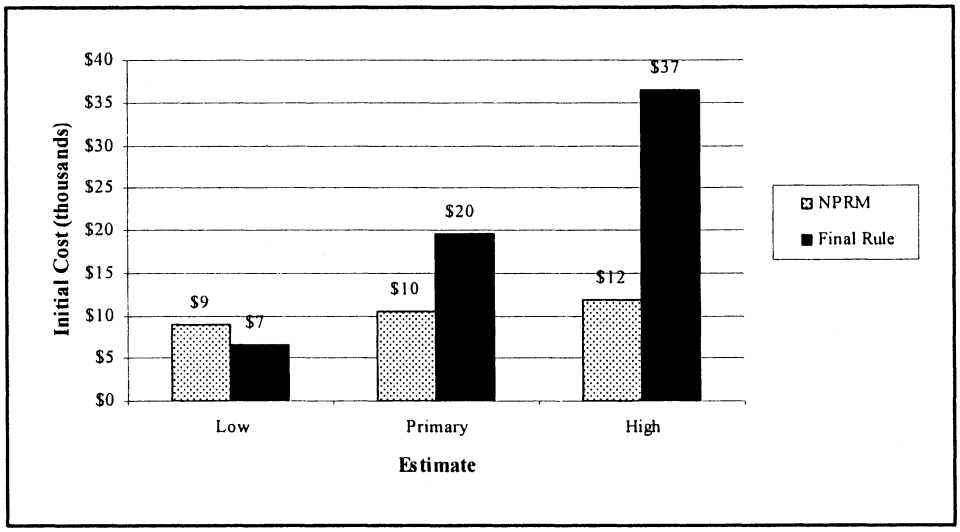
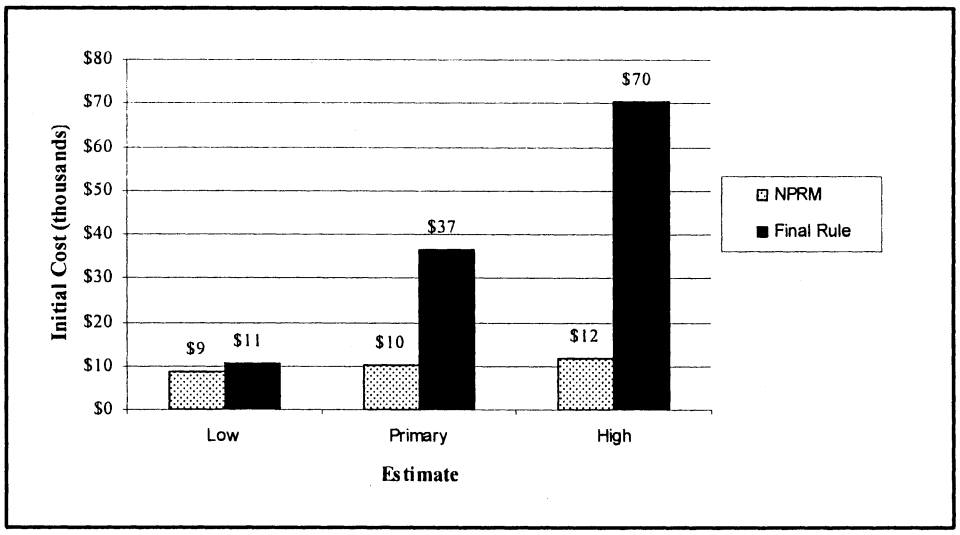


Table 9 shows how we adjusted our low, primary, and high initial compliance cost estimates for small facilities from the NPRM estimates included in the IRFA. Again, the change in cost estimates is principally the result of modifications to our estimates for facilities to provide escorted access to employees and visitors who do not have unescorted access authority. (As there are no small entities that operate facilities on the OCS, we did not estimate compliance costs for these firms under the FRFA.)

Table 9: Difference in Initial Cost Estimate for Small Facilities



Even though we have determined that this rule will have a significant economic impact on a substantial number of small entities, we also believe that the rule provides small entities with a significant amount of flexibility to achieve the requirements of the regulation.

First, and perhaps most importantly, the final rule no longer requires the use of biometric smart card readers by vessels, facilities, and OCS facilities. This should substantial decrease the burden on small entities, as there is no new capital investment required under this rulemaking. Additionally, the Coast Guard will conduct spot checks with hand held readers to ensure that individuals and regulated entities are utilizing the TWIC in a fashion consistent with the requirements of the rule. By completing these checks, the Coast Guard will be able verify the identity of TWIC holders, as well as confirm the validity of their credentials. This should also serve to lower the regulatory burden on small entities by transitioning some of the cost of TWIC verifications to the Federal government.

The recordkeeping requirement proposed in the NPRM has also been dropped from the final rule, as has the requirement for firms to submit TWIC addenda. These alterations should also decrease the cost of compliance to small entities.

The provision for passenger access areas, which we originally proposed in the NPRM for passenger vessels, remains in the final rule and provides flexibility for small entities offering services to passengers. MTSA provides that no one may have unescorted access to secure areas unless they carry a

TWIC. To ensure that passenger vessels do not have to require passengers to obtain TWICs or ensure that passengers are ''escorted'' at all times while on the vessel, the rule creates the ''passenger access area,'' allowing vessel owners/operators to carve out areas within the secure areas aboard their vessels where passengers are free to move about unescorted.

In addition to the passenger access areas, the final rule creates ''employee access areas,'' allowing passenger vessel and ferry owners/operators more flexibility. An employee access area is a defined space within the access control area of a ferry or passenger vessel that is open to employees but not passengers. It is not a secure area and does not require a TWIC for unescorted access. It may not include any areas defined as restricted areas in the vessel security plan. We believe that this new provision should reduce the regulatory burden on many small passenger vessels, especially those that primarily utilize and rely on seasonal labor.

The final rule also includes a new provision that will allow a direct hire new employee to receive limited access to secure areas of a vessel or facility, provided that both the new employee and the owner/operator meet certain stipulations, which are detailed in the regulatory text. This new policy, which TSA and the Coast Guard did not propose in the NPRM, is intended to give owners/operators the flexibility to quickly give new employees who do not yet hold a TWIC access to secure areas.

In addition to making accommodations for new hires, the final rule also includes a provision for individuals who have reported their credential as either lost, damaged, or stolen. Although the provision contains certain caveats that are specified in the regulatory text, this new policy allows an employee missing or unable to use his or her credential to receive limited unescorted access to secure areas, including restricted areas, for seven calendar days.

Further, the final rule also allows certain facilities to submit amendments to their security plans in order to redefine their access control areas, which in turn may reduce their secure areas. By allowing small facilities to more closely focus their access control areas on a portion of their facility directly related to maritime transportation, this may reduce the rule's economic impact on small entities.

Finally, in an effort to maintain security but ensure applicants' rights, the rule now also allows for review by an ALJ in cases where TSA denies a waiver request. Moreover, the final rule extends the response time for applicants to appeal an adverse determination, correct an open criminal disposition, or apply for a waiver to 60 days. In addition, individuals, such as mariners who are at sea for extended periods of time, who legitimately miss the 60-day response time period may petition TSA to reconsider an Initial Determination.

TSA and the Coast Guard believe the policies outlined above provide small entities with flexibility in complying with the rule. We believe the final rule minimizes the adverse economic effects to small business while fulfilling all statutory requirements, as well as TSA's and the Coast Guard's primary objective of increased security.

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121), we want to assist small entities in understanding this proposed rule so that they can better evaluate its effects on them and participate in the rulemaking. If the rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult LCDR Jonathan Maiorine, Commandant (G–PCP–2), United States Coast Guard, 2100 Second Street, SW., Washington, DC 20593; telephone 1 (877) 687–2243. DHS will not retaliate against small entities that question or complain about this rule or any policy or action of DHS.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of TSA or of the Coast Guard, call 1–888–REG–FAIR (1–888–734–3247).

D. Collection of Information

This rule would call for a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520). As defined in 5 CFR 1320.3(a), ''collection of information'' includes reporting, recordkeeping, monitoring, posting, labeling, and other, similar actions. The title and description of the information collections, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for reviewing instructions, searching existing sources of data, gathering and maintaining the data needed, and completing and reviewing the collection.

Title: Transportation Worker Identification Credential (TWIC) Program.

Summary of the Collection of Information:

Need for Information: TSA has developed the Transportation Worker Identification Credential (TWIC) as an identification tool that encompasses the authorities of the Aviation and Transportation Security Act of 2001 (ATSA) (Pub. L. 107–71, Sec. 106), and the Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. 107–295, Sec. 102) to perform background checks and issue credentials to workers within the national transportation system. The data to be collected is that biographic and biometric information necessary for TSA to complete the required security threat assessment on individuals who will seek unescorted access to secure areas of vessels and maritime facilities through the use of a TWIC. TWIC cards, when issued, will contain biographic and biometric data necessary to prove identity of the cardholder and to interoperate with access control systems on vessels and at facilities nationwide.

Proposed Use of Information: TSA will use the information to verify the identity of the individual applying for a TWIC and to verify that the person poses no security threat that would preclude issuance of a TWIC.

Description of the Respondents: The respondents to this collection of information will be workers within the national transportation system, specifically individuals who require unescorted access to secure areas of vessels or maritime facilities.

Number of Respondents: Although the number of respondents will vary over three years, TSA estimates that the annualized number of total respondents will be approximately 317,400. Based on research conducted by TSA and the Coast Guard, the total estimated base population that will be affected by TWIC is 750,000. However, TSA estimates that more than seventy percent of the base maritime worker population will enroll in the program in the first year, and the remainder will enroll in year two. Turnover and growth within the affected population is expected to result in another 202,257 respondents.

Frequency of Response: Because renewals for the TWIC will be on a five year basis, for purposes of the Paperwork Reduction Act, to apply for a TWIC, each respondent will be

required to respond once to the enrollment collection. TSA estimates an additional response from the estimated two percent of respondents who will appeal decisions made by the agency with respect to security threat assessments or ask for a waiver from disqualifying offenses. Thus, TSA estimates the number of total annual responses to be approximately 323,800.

Burden of Response: TSA estimates the annual hour burden for enrollment to be 476,129, or one and one half hour per respondent. TSA estimates the annual hour burden for appeals and waiver to be approximately 38,100.

TSA has determined that the information collection and card issuance portion of the TWIC fee will be between $45 and $65 per respondent. This portion of the fee accounts for more than the actual cost of the information collection as it includes cost of the enrollment process, system operations and maintenance, and TWIC distribution.

Estimate of Total Annual Burden: TSA estimates the total annual hour burden as a result of this collection of information to be approximately 514,200. Because the TWIC fee may change over time as actual costs are determined and annualized, TSA estimates total annual fee for respondents to be between $14,283,855 and $20,632,235.

As required by the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3507(d)), we have submitted a copy of this proposed rule to the Office of Management and Budget (OMB) for its review of the collection of information.

The provisions contained in the amendments to Title 33 do not call for a new collection of information under the PRA (44 U.S.C. 3501–3520). While they include potential amendments of vessel or facility security plans, these amendments are covered by an approved collection of information. The approval number from OMB is OMB Control Number(s) 1625–0077 ''Security Plan for Ports, Vessels, Facilities, Outer Continental Shelf Facilities and Other Security-Related Requirements,'' which expires on July 31, 2008.

The new hire provision requirements affecting Homeport will be added to collection 1625–0110 ''Maritime Identification Credentials—Title 33 CFR Part 125'', which expired on November 30, 2006. The three year renewal for 1625–0110 was submitted to OMB on October 6, 2006 and an amendment to that renewal reflecting the proposed changes due to the new hire provisions was submitted to OMB on December 29, 2006. The revision would change the collection, once the TWIC program goes into effect, to make the submission of new hire information voluntary and require owners and operators to receive a positive verification from Homeport prior to granting access to the new hire. The government's need for the information, the type of information to be submitted, the method of submission, and the frequency of submission should not change from the current collection.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. Before the requirements for this collection of information become effective, we will publish a Notice in the **Federal Register** of OMB's decision to approve, modify, or disapprove the collection.

E. Executive Order 13132 (Federalism)

A rule has implications for federalism under E.O. 13132, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. TSA and Coast Guard have analyzed this final rule under that Order and have determined that it has implications for federalism, for the same reasons that we found federalism impacts for the Coast Guard's previously published MTSA regulations. 68 FR at 60468–9. A summary of the impacts on federalism in this rule follows.

This rule would have a substantial direct effect on States, local governments, or political subdivisions under section 1(a) of the Order when those states owning vessels/facilities are required to implement a TWIC program. It would also preempt State law under section 6(c) of the Order by: Continuing to prevent States from regulating mariners; and continuing to prevent the States from requiring security plans.

Regulations already issued by the Coast Guard under other sections of the MTSA of 2002 cited the need for national standards of security, claimed preemption, and received comments in support of such a scheme. *See,* 68 FR 60448, 60468–60469. (October 23, 2003).

The law is well-settled that States may not regulate in categories expressly reserved for regulation by the Coast Guard. The law also is well-settled that all of the categories covered in 46 U.S.C. 3306, 3703, 7101, and 8101 (design, construction, alteration, repair, maintenance, operation, equipping, personnel qualification, and manning of vessels), as well as the reporting of casualties and any other category in which Congress intended the Coast Guard to be the sole source of a vessel's obligations, are within the field foreclosed from regulation by the States. *See United States* v. *Locke* and *Intertanko* v. *Locke,* 529 U.S. 89 (2000). Since portions of this proposed rule involve the manning of U.S. vessels and the licensing of merchant mariners, it relates to personnel qualifications. Because the states may not regulate within this category, these portions of this rule do not present new preemption issues under E.O. 13132.

We are only asserting field preemption in those areas where federal regulations have historically dominated the field, such as merchant mariner regulations, or where we are amending regulations that we have previously preempted state regulation, such as the MTSA regulations found in 33 CFR chapter I, subchapter H. States would not be preempted from instituting their own background checks or badging systems in addition to the TWIC.

Some commenters objected to allowing State or local governments to impose credentialing or background check requirements, noting that it results in multiple background checks for workers. We have carefully considered whether State and local governments should be preempted from doing so, and have determined that we are not preempting such State and local activities.

Under this rulemaking, States will not be preempted from instituting their own background checks or badging systems in addition to the TWIC. We note that a State may be the proprietor of ports or port facilities, and as the proprietor is free to set standards for who may enter onto their facilities, as does any other proprietor. In addition, States may have set standards for reasons other than guarding against the threat of terrorism, such as to combat drug smuggling or organized crime. As such they are not regulating in the areas that DHS is regulating.

The Department has also considered an additional federalism matter with respect to the TWIC credential. Section 102 of MTSA, 46 U.S.C. 70105, contains no express exceptions for State and local officials. As noted earlier in this preamble, however, the Department will not with this final rule require State and local officials to obtain a TWIC credential prior to their unescorted access to the ports. The Department's decision reflects the concern that denying port access to State and local officials, including law enforcement officials, may have serious federalism implications, particularly where there is not sufficient evidence of Congress's intent to do so. State law enforcement officials, for example, have authority and emergency aid responsibilities in

and around ports pursuant to laws properly promulgated by State legislatures and consistent with historic State police powers. The incidental application to these State officials of the MTSA's generally applicable requirements—for example, by barring them from secure areas of ports unless they obtain a federal credential—may excessively interfere with the functioning of State governments. *Cf. Printz* v. *United States,* 521 U.S. 898, 932 (1997); *see also Gregory* v. *Ashcroft,* 501 U.S. 452, 460 (1991) (emphasizing importance of State power to prescribe qualifications of its own officials. ''Through the structure of its government and the character of those who exercise government authority, a State defines itself as a sovereign''). We are hesitant to impose such a requirement on State and local governments when Congress has not made its intention in this respect clear and manifest. *See Rice* v. *Santa Fe Elevator Corp.,* 331 U.S. 218, 230 (1947). The decision to exempt State and local officials from the TWIC requirements thus maintains the role of State and local officials in areas traditionally under their jurisdiction.

F. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100,000,000 or more in any one year. This rule would result in such an expenditure for the private sector, and we discuss the effects of this rule in the Final Regulatory Assessment, which is summarized in the E.O. 12866 section above.

G. Taking of Private Property

This rule would not affect a taking of private property or otherwise have taking implications under E.O. 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights.

H. Civil Justice Reform

This rule meets applicable standards in sections 3(a) and 3(b)(2) of E.O. 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden.

I. Protection of Children

We have analyzed this rule under E.O. 13045, Protection of Children from Environmental Health Risks and Safety Risks. While this rule is an economically significant rule, it would not create an environmental risk to health or safety that might disproportionately affect children.

J. Indian Tribal Governments

This rule does not have tribal implications under E.O. 13175, Consultation and Coordination with Indian Tribal Governments, because it would not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

K. Energy Effects

We have analyzed this rule under E.O. 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use. We have determined that it is not a ''significant energy action'' under that order. While it is a ''significant regulatory action'' under E.O. 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy. The Administrator of the Office of Information and Regulatory Affairs has not designated it as a significant energy action. Therefore, a Statement of Energy Effects is not required for this rule under E.O. 13211.

One commenter disagreed with this statement, stating that any significant new regulation of the transportation system will significantly affect the distribution system, particularly in the short term. The commenter requested a delay in the effective date of the rule along with a longer time period to ensure full compliance with the program. The commenter expressed doubt that there will be an adequate supply of TWIC readers available, adding that the regulations must allow companies to operate until the TWIC system is installed and usable.

We disagree with the commenter. The original MTSA regulations were also a significant new regulation of the maritime transportation system, and we did not see a significant effect on the energy distribution system during the implementation of those regulations. However, we note that the intent of this commenter is being satisfied, as the reader requirements have not been included in the final rule.

L. Technical Standards

The National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. 272 note) directs agencies to use voluntary consensus standards in their regulatory activities unless the agency provides Congress, through the OMB, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (*e.g.,* specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies.

While the NPRM proposed incorporating a standard, this rule does not. Therefore, we did not consider the use of voluntary consensus standards for this final rule.

M. Environment

The Transportation Worker Identification Credential (TWIC) rule contains a program of activities to improve the safety and security of vessels, facilities, OCS facilities, and U.S. ports. It establishes requirements for secure identification cards, developing application forms, collecting and processing forms, application evaluation criteria, issuing determinations on applications, and use of the identification cards to enhance security at MTSA-regulated facilities and vessels. It will contribute to a higher level of marine safety and security for vessels, facilities, OCS facilities, and U.S. ports.

Initially, implementation of this rule will involve establishing ''enrollment stations'' to collect TWIC applications. The enrollment stations will include a small office, using existing utilities where possible, located in space made available in existing port facilities or other available space within a 25 mile radius of the port facility. If a location does not have a port facility, or enough space, a temporary unit will be provided until either sufficient permanent space is available or the need for the enrollment station no longer exists. To meet the initial surge of enrollments expected, approximately 130 stations (permanent and mobile/temporary) are expected to be operating nationwide. The ongoing/maintenance phase will involve approximately 134 stations.

Once the initial enrollment period is complete and TWICs have been issued to maritime personnel, implementation will involve an inspection of the TWIC by the vessel or facility owner/operator for a worker to gain unescorted access to secure areas of vessels and facilities. The inspection of the TWIC must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to ensure that the TWIC has not been forged or tampered.

There are preexisting requirements in 46 U.S.C. 70103(c)(3)(C) and in 33 CFR part 125 that require waterfront facilities and vessels to maintain security plans that implement access control measures including the use of appropriate identification credentials. In addition, current regulations at 33 CFR part 101 establish federal identification standards. At some seaports, States and port operators have also established identification requirements. States and port operators have the option to either replace their existing identification requirements with the TWIC or to maintain their existing identification requirements in addition to the TWIC. In either case, inspection of the TWIC is not expected to add significant time to the entry procedures at any seaport.

The provisions of this rule have been analyzed under the Department of Homeland Security (DHS) Management Directive (MD) 5100.1, Environmental Planning Program, which is the DHS policy and procedures for implementing the National Environmental Policy Act (NEPA), and related E.O.s and requirements. Based on a review of current practices and expected changes that would result from this rule, there would be no significant environmental impact in requiring those entering the port facility to display the TWIC card in addition to or as a substitute for their regular identification as a flash pass. There are no extraordinary circumstances presented by this rule that would limit the use of a CATEX under MD 5100.1, Appendix A, paragraph 3.2. The implementation of this rule is categorically excluded under the following categorical exclusions (CATEX) listed in MD 5100.1, Appendix A, Table 1: CATEX A1 (personnel, fiscal, management and administrative activities); CATEX A3 (promulgation of rules, issuance of rulings or interpretations); and CATEX A4 (information gathering, data analysis and processing, information dissemination, review, interpretation and development of documents). CATEX B3 (proposed activities and operations to be conducted in an existing structure that would be compatible with and similar in scope to ongoing functional uses) and CATEX B 11 (routine monitoring and surveillance activities that support law enforcement or homeland security and defense operations) would also be applicable.

VI. Solicitation of Comments

TSA is soliciting public comments on the card replacement fee. The NPRM estimated that the card replacement fee would be $36. Since issuance of the NPRM, TSA has learned that the costs associated with replacing the card will be higher than anticipated. In this preamble, an explanation of the differences appears in section I, Background, under Fees. TSA now estimates that it will cost TSA $60 per card to issue replacements. Because this cost is significantly higher than proposed, TSA invites public comment on this issue. This Final Rule establishes the card replacement fee at $36. TSA will issue cards at the $36.00 fee but proposes to increase this fee to $60. TSA invites comment on the proposed increase of the Card Replacement Fee.

List of Subjects

33 CFR Part 101

Harbors, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

33 CFR Part 103

Facilities, Harbors, Maritime security, Ports, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

33 CFR Part 104

Incorporation by reference, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels.

33 CFR Part 105

Facilities, Maritime security, Reporting and recordkeeping requirements, Security measures.

33 CFR Part 106

Facilities, Maritime security, Outer Continental Shelf, Reporting and recordkeeping requirements, Security measures.

33 CFR Part 125

Administrative practice and procedure, Harbors, Reporting and recordkeeping requirements, Security measures, Vessels.

46 CFR Part 10

Penalties, Reporting and recordkeeping requirements, Schools, Seamen.

46 CFR Part 12

Penalties, Reporting and recordkeeping requirements, Seamen.

46 CFR Part 15

Reporting and recordkeeping requirements, Seamen, Vessels.

49 CFR Part 1515

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

49 CFR Part 1540

Air carriers, Airports, Aviation safety, Law enforcement officers, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1570

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

49 CFR Part 1572

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

The Amendments

■ For the reasons listed in the preamble, the Coast Guard amends 33 CFR parts 101, 103, 104, 105, 106, 125; and 46 CFR parts 10, 12, and 15 and the Transportation Security Administration adds or amends 49 CFR parts 1515, 1570, and 1572 as follows:

Title 33—Navigation and Navigable Waters

CHAPTER I—COAST GUARD

PART 101—MARITIME SECURITY: GENERAL

■ 1. The authority citation for part 101 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

■ 2. In § 101.105 add, in alphabetical order, definitions for the terms escorting, personal identification number (PIN), recurring unescorted access, secure area, TWIC, TWIC

program, and unescorted access, to read as follows:

§ 101.105 Definitions.

* * * * *

Escorting means ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted. This may be accomplished via having a side-by-side companion or monitoring, depending upon where the escorted individual will be granted access. Individuals without TWICs may not enter restricted areas without having an individual who holds a TWIC as a side-by-side companion, except as provided in §§ 104.267, 105.257, and 106.262 of this subchapter.

* * * * *

Personal Identification Number (PIN) means a personally selected number stored electronically on the individual's TWIC.

* * * * *

Recurring unescorted access means authorization to enter a vessel on a continual basis after an initial personal identity and credential verification.

* * * * *

Secure Area means the area on board a vessel or at a facility or outer continental shelf facility over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard approved security plan. It does not include passenger access areas, employee access areas, or public access areas, as those terms are defined in §§ 104.106, 104.107, and 105.106, respectively, of this subchapter. Vessels operating under the waivers provided for at 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. Facilities subject to part 105 of this subchapter may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure areas.

* * * * *

TWIC means a valid, non-revoked transportation worker identification credential, as defined and explained in 49 CFR part 1572.

TWIC Program means those procedures and systems that a vessel, facility, or outer continental shelf facility (OCS) must implement in order to assess and validate TWICs when maintaining access control.

* * * * *

Unescorted access means having the authority to enter and move about a secure area without escort.

* * * * *

■ 3. Add § 101.514 to read as follows:

§ 101.514 TWIC Requirement.

(a) All persons requiring unescorted access to secure areas of vessels, facilities, and OCS facilities regulated by parts 104, 105 or 106 of this subchapter must possess a TWIC before such access is granted, except as otherwise noted in this section. A TWIC must be obtained via the procedures established by TSA in 49 CFR part 1572.

(b) Federal officials are not required to obtain or possess a TWIC. Except in cases of emergencies or other exigent circumstances, in order to gain unescorted access to a secure area of a vessel, facility, or OCS facility regulated by parts 104, 105 or 106 of this subchapter, a federal official must present his/her agency issued, HSPD 12 compliant credential. Until each agency issues its HSPD 12 compliant cards, Federal officials may gain unescorted access by using their agency's official credential. The COTP will advise facilities and vessels within his or her area of responsibility as agencies come into compliance with HSPD 12.

(c) Law enforcement officials at the State or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas. They may, however, voluntarily obtain a TWIC where their offices fall within or where they require frequent unescorted access to a secure area of a vessel, facility or OCS facility.

(d) Emergency responders at the State, or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas during an emergency situation. They may, however, voluntarily obtain a TWIC where their offices fall within or where they desire frequent unescorted access to a secure area of a vessel, facility or OCS facility in non-emergency situations.

(e) Before September 25, 2008, mariners do not need to obtain or possess a TWIC but may be provided unescorted access to secure areas of vessels, facilities, and OCS facilities regulated by parts 104, 105 or 106 of this subchapter if they are able to show one of the following:

(1) A valid Merchant Mariner Document (MMD);

(2) A valid Merchant Mariner License and a valid photo identification; or

(3) A valid Certificate of Registry and a valid photo identification.

■ 4. Revise § 101.515 to read as follows:

§ 101.515 TWIC/Personal Identification.

(a) Persons not described in § 101.514 of this part shall be required to present personal identification in order to gain entry to a vessel, facility, and OCS facility regulated by parts 104, 105 or 106 of this subchapter. These individuals must be under escort, as that term is defined in § 101.105 of this part, while inside a secure area. This personal identification must, at a minimum, meet the following requirements:

(1) Be laminated or otherwise secure against tampering;

(2) Contain the individual's full name (full first and last names, middle initial is acceptable);

(3) Contain a photo that accurately depicts that individual's current facial appearance; and

(4) Bear the name of the issuing authority.

(b) The issuing authority in paragraph (a)(4) of this section must be:

(1) A government authority, or an organization authorized to act of behalf of a government authority; or

(2) The individual's employer, union, or trade association.

(c) Vessel, facility, and OCS facility owners and operators must permit law enforcement officials, in the performance of their official duties, who present proper identification in accordance with this section and § 101.514 of this part to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel, facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.

(d) *Inspection of credential.* (1) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(2) Each person who has been issued or who possesses a TWIC must allow his or her TWIC to be read by a reader and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a PIN, to the reader, upon a request from TSA, the Coast Guard, other authorized DHS representative; or a Federal, State, or local law enforcement officer.

PART 103—MARITIME SECURITY: AREA MARITIME SECURITY

■ 5. The authority citation for part 103 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70102, 70103, 70104, 70112; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

■ 6. Revise § 103.305(c) to read as follows:

§ 103.305 Composition of an Area Maritime Security (AMS) Committee.

* * * * *

(c) Members appointed under this section serve for a term of not more than five years. In appointing members, the FMSC should consider the skills required by § 103.410 of this part. With the exception of credentialed Federal, state and local officials, all AMS Committee members shall have a name-based terrorist check from TSA, hold a TWIC, or have passed a comparable security threat assessment, if they need access to SSI as determined by the FMSC.

■ 7. Revise § 103.505(f) to read as follows:

§ 103.505 Elements of the Area Maritime Security (AMS) plan.

* * * * *

(f) Measures to prevent unauthorized access to designated restricted areas within the port (e.g., TWIC);

* * * * *

PART 104—MARITIME SECURITY: VESSELS

■ 8. The authority citation for part 104 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

■ 9. Amend § 104.105 by redesignating paragraph (d) as paragraph (f) and adding new paragraphs (d) and (e) to read as follows:

§ 104.105 Applicability.

* * * * *

(d) The TWIC requirements found in this part do not apply to foreign vessels.

(e) The TWIC requirements found in this part do not apply to mariners employed aboard vessels moored at U.S. facilities only when they are working immediately adjacent to their vessels in the conduct of vessel activities.

* * * * *

■ 10. Add § 104.106 to read as follows:

§ 104.106 Passenger access area.

(a) A ferry, passenger vessel, or cruise ship may designate areas within the vessel as passenger access areas.

(b) A passenger access area is a defined space, within the area over which the owner or operator has implemented security measures for access control, of a ferry, passenger vessel, or cruise ship that is open to passengers. It is not a secure area and does not require a TWIC for unescorted access.

■ 11. Add § 104.107 to read as follows:

§ 104.107 Employee access area.

(a) A ferry or passenger vessel, excluding cruise ships, may designate areas within the vessel as employee access areas.

(b) An employee access area is a defined space, within the area over which the owner or operator has implemented security measures for access control, of a ferry or passenger vessel that is open only to employees and not to passengers. It is not a secure area and does not require a TWIC for unescorted access.

(c) Employee access areas may not include any areas defined as restricted areas in the VSP.

■ 12. Amend § 104.115 by adding paragraphs (c) and (d) to read as follows:

§ 104.115 Compliance dates.

* * * * *

(c) Persons required to obtain a TWIC under this part may enroll beginning after the date set by the Coast Guard in a Notice to be published in the **Federal Register**. This notice will be directed to all facilities and vessels within a specific COTP zone.

(d) By September 25, 2008, vessel owners or operators subject to paragraph (b) of this section and not excluded by § 104.105(d) of this part must be operating in accordance with the TWIC provisions found within this part.

■ 13. Amend § 104.120 by adding paragraph (c) to read as follows:

§ 104.120 Compliance documentation.

* * * * *

(c) Each vessel owner or operator who designates a passenger or employee access area (as those terms are defined in §§ 104.106 and 104.107 of this part) on their vessel must keep on board the vessel with their approved VSP a clear, visual representation (such as a vessel schematic) of where those designated areas fall. This need not be submitted to the Coast Guard for approval until incorporated into the VSP at the next VSP submittal (either renewal or amendment), but must be made available to the Coast Guard upon request.

Subpart B—Vessel Security Requirements

■ 14. Revise § 104.200(b) to read as follows:

§ 104.200 Owner or operator.

* * * * *

(b) For each vessel, the vessel owner or operator must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Designate, in writing, by name or title, a Company Security Officer (CSO), a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;

(3) Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;

(4) Inform vessel personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(5) Ensure vessel security records are kept;

(6) Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DoS);

(7) Ensure coordination of shore leave, transit, or crew change-out for vessel personnel, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival. Vessel owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations in coordinating such leave. The text of these treaties can be found at *http://www.marad.dot.gov/Programs/treaties.html;*

(8) Ensure security communication is readily available;

(9) Ensure coordination with and implementation of changes in Maritime Security (MARSEC) Level;

(10) Ensure that security systems and equipment are installed and maintained;

(11) Ensure that vessel access, including the embarkation of persons and their effects, is controlled;

(12) Ensure that TWIC procedures are implemented as set forth in this part, including;

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in secure areas are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Notifying vessel employees, and passengers if applicable, of what parts of the vessel are secure areas, employee access areas, and passenger access areas, as applicable, and ensuring such areas are clearly marked.

(13) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(14) Ensure that protocols consistent with § 104.265(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place;

(15) Ensure that cargo and vessel stores and bunkers are handled in compliance with this part;

(16) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

(17) Provide the Master, or for vessels on domestic routes only, the CSO, with the following information:

(i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractors, concessionaires (for example, retail sales outlets, casinos, etc.);

(ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and

(iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and

(18) Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods; and

(19) If applicable, ensure that protocols consistent with § 104.267 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

■ 15. Amend § 104.210 by adding paragraphs (a)(5), (b)(2)(xv) and (c)(15) to read as follows:

§ 104.210 Company Security Officer (CSO).

(a) * * *

(5) The CSO must maintain a TWIC.

(b) * * *

(2) * * *

(xv) Knowledge of TWIC requirements

(c) * * *

(15) Ensure the TWIC program is being properly implemented.

■ 16. Amend § 104.215 by adding paragraphs (a)(6), (b)(7) and (c)(12) to read as follows:

§ 104.215 Vessel Security Officer (VSO).

(a) * * *

(6) The VSO must maintain a TWIC.

(b) * * *

(7) TWIC

(c) * * *

(12) Ensure TWIC programs are in place and implemented appropriately.

■ 17. Amend § 104.220 by revising the introductory paragraph and adding paragraph (n) to read as follows:

§ 104.220 Company or vessel personnel with security duties.

Company and vessel personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(n) Relevant aspects of the TWIC program and how to carry them out.

■ 18. Amend § 104.225 by adding paragraph (f) to read as follows:

§ 104.225 Security training for all other personnel.

* * * * *

(f) Relevant aspects of the TWIC program and how to carry them out.

■ 19. Revise § 104.265 to read as follows:

§ 104.265 Security measures for access control.

(a) *General.* The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board;

(3) Control access to the vessel; and

(4) Prevent an unescorted individual from entering an area of the vessel that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

(b) The vessel owner or operator must ensure that the following are specified:

(1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level, including those points where TWIC access control provisions will be applied. ''Means of access'' include, but are not limited, to all:

(i) Access ladders;

(ii) Access gangways;

(iii) Access ramps;

(iv) Access doors, side scuttles, windows, and ports;

(v) Mooring lines and anchor chains; and

(vi) Cranes and hoisting gear;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and procedures for escorting, in accordance with § 101.515 of this subchapter; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The vessel owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with § 101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the vessel and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than seven consecutive calendar days provided that:

(i) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of § 101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside a secure area.

(4) With the exception of persons granted access according to paragraph (2) of this section, all persons granted unescorted access to secure areas of the vessel must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The vessel's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of facilities or other transportation conveyances that interface with the vessel.

(d) If the vessel owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The vessel owner or operator must establish in the approved VSP the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.

(f) *MARSEC Level 1.* The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Employ TWIC as set out in paragraph (c) of this section.

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Boarding the vessel is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to board;

(4) Check the identification of any person not holding a TWIC and seeking to board the vessel, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the vessel;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(9) Provide a designated area on board, within the secure area, or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;

(10) Ensure vessel personnel are not subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it;

(11) Conduct screening in a way that takes into full account individual human rights and preserves the individual's basic human dignity;

(12) Ensure the screening of all unaccompanied baggage;

(13) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;

(14) Ensure embarking passengers are segregated from disembarking passengers;

(15) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;

(16) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading; and

(17) Respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.

(g) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2 in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(4) Limiting the number of access points to the vessel by closing and securing some access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols; and

(7) Establishing a restricted area on the shore side of the vessel, in close cooperation with the facility.

(h) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. The additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively, for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage on board;

(3) Being prepared to cooperate with responders and facilities;

(4) Limiting access to the vessel to a single, controlled access point;

(5) Granting access to only those responding to the security incident or threat thereof;

(6) Suspending embarkation and/or disembarkation of personnel;

(7) Suspending cargo operations;

(8) Evacuating the vessel;

(9) Moving the vessel; or

(10) Preparing for a full or partial search of the vessel.

■ 20. Add § 104.267 to read as follows:

§ 104.267 Security measures for newly hired employees.

(a) Newly-hired vessel employees may be granted entry to secure areas of the vessel for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the vessel. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may

further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired vessel employees may be granted the access provided for in paragraph (a) of this section only if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The vessel owner or operator or Vessel Security Officer (VSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The vessel owner or operator or the VSO enters the following information on the new hire into the Coast Guard's Homeport website (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment;

(3) The new hire presents an identification credential that meets the requirements of § 101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the vessel owner or operator or VSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to vessel operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a Company Security Officer (CSO) or VSO, or any individual being hired to perform vessel security duties.

(d) The new hire may not begin working on board the vessel under the provisions of this section until the owner, operator, or VSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

Subpart D—Vessel Security Plan (VSP)

■ 21. Revise § 104.405(a)(10) and (b) to read as follows:

§ 104.405 Format of the Vessel Security Plan (VSP).

(a) * * *

(10) Security measures for access control, including designated passenger access areas and employee access areas;

* * * * *

(b) The VSP must describe in detail how the requirements of subpart B of this part will be met. VSPs that have been approved by the Coast Guard prior to March 26, 2007, do not need to be amended to describe their TWIC procedures until the next regularly scheduled resubmission of the VSP.

PART 105—MARITIME SECURITY: FACILITIES

■ 22. The authority citation for part 105 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

■ 23. Amend § 105.115 by adding paragraphs (c), (d), and (e) to read as follows:

§ 105.115 Compliance dates.

* * * * *

(c) Facility owners or operators wishing to designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure area(s) must do so by submitting an amendment to their Facility Security Plan to their cognizant COTP, in accordance with § 105.415 of this part, by July 25, 2007.

(d) Persons required to obtain a TWIC under this part may enroll beginning after the date set by the Coast Guard in a Notice to be published in the **Federal Register**. This notice will be directed to all facilities and vessels within a specific COTP zone.

(e) Facility owners or operators must be operating in accordance with the TWIC provisions in this part by the date set by the Coast Guard in a Notice to be published in the **Federal Register**. This Notice will be published at least 90 days before compliance must begin, and will be directed to all facilities within a specific Captain of the Port zone, based on whether enrollment has been completed in that zone. Unless an earlier compliance date is specified in this manner, all facility owner or operators will need to implement their TWIC provisions no later than September 25, 2008.

Subpart B—Facility Security Requirements

■ 24. Revise § 105.200(b) to read as follows:

§ 105.200 Owner or operator.

* * * * *

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of an FSP;

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including:

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the secure area in accordance with the FSP are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Notifying facility employees, and passengers if applicable, of what parts of the facility are secure areas and public access areas, as applicable, and ensuring such areas are clearly marked.

(7) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(8) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(9) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can be found at *http://www.marad.dot.gov/Programs/treaties.html;*

(10) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(11) Ensure security for unattended vessels moored at the facility;

(12) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter;

(13) Ensure consistency between security requirements and safety requirements;

(14) Inform facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(15) Ensure that protocols consistent with section 105.255(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place; and

(16) If applicable, ensure that protocols consistent with § 105.257 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

■ 25. Amend § 105.205 by adding paragraphs (a)(4), (b)(2)(xv) and (c)(19) to read as follows:

§ 105.205 Facility Security Officer (FSO).

(a) * * *

(4) The FSO must maintain a TWIC.

(b) * * *

(2) * * *

(xv) Knowledge of TWIC requirements.

(c) * * *

(19) Ensure the TWIC program is being properly implemented.

■ 26. Amend § 105.210 by revising the introductory paragraph and adding paragraph (n) to read as follows:

§ 105.210 Facility personnel with security duties.

Facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(n) Familiar with all relevant aspects of the TWIC program and how to carry them out.

■ 27. Amend § 105.215 by adding paragraph (f) to read as follows:

§ 105.215 Security training for all other facility personnel.

* * * * *

(f) Familiar with all relevant aspects of the TWIC program and how to carry them out.

■ 28. Revise § 105.255 to read as follows:

§ 105.255 Security measures for access control.

(a) *General.* The facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility;

(3) Control access to the facility; and

(4) Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

(b) The facility owner or operator must ensure that the following are specified:

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level, including those points where TWIC access control provisions will be applied. Each location allowing means of access to the facility must be addressed;

(2) The types of restrictions or prohibitions to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC, in accordance with § 101.515 of this subchapter, and procedures for escorting them;

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level; and

(5) The locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

(c) The facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with § 101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if:

(i) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of § 101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside of a secure area.

(4) With the exception of persons granted access according to paragraph (c)(2) of this section, all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.

(d) If the facility owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) *MARSEC Level 1.* The facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section.

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter.

(4) Check the identification of any person not holding a TWIC and seeking entry to the facility, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check shall include confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.

(5) Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence. Any such incident must be reported in compliance with this part;

(6) Designate restricted areas and provide appropriate access controls for these areas;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(9) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(10) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(g) *MARSEC Level 2*. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(h) *MARSEC Level 3*. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling of unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage.

(3) Being prepared to cooperate with responders and facilities;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

■ 28. Add § 105.257 to read as follows:

§ 105.257 Security measures for newly-hired employees.

(a) Newly-hired facility employees may be granted entry to secure areas of the facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the facility. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired facility employees may be granted the access provided for in paragraph (a) of this section if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The facility owner or operator or the Facility Security Officer (FSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport website (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment.

(3) The new hire presents an identification credential that meets the requirements of § 101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the facility owner or operator or FSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to facility operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a FSO, or any individual being hired to perform facility security duties.

(d) The new hire may not begin working at the facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

■ 29. Amend § 105.285 by revising paragraph (a)(4) to read as follows:

§ 105.285 Additional requirements—passenger and ferry facilities.

(a) * * *

(4) Deny passenger access to secure and restricted areas unless escorted by

authorized facility security personnel; and

* * * * *

■ 30. Revise § 105.290 to read as follows:

§ 105.290 Additional requirements—cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

(a) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(b) Check the identification of all persons seeking to enter the facility. Persons holding a TWIC shall be checked as set forth in this part. For persons not holding a TWIC, this check includes confirming the reason for boarding by examining passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(c) Designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects awaiting embarkation from unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area; and

(e) Deny individuals not holding a TWIC access to secure and restricted areas unless escorted.

■ 31. Amend § 105.296 by adding paragraph (a)(4) to read as follows:

§ 105.296 Additional requirements—barge fleeting facilities.

(a) * * *

(4) Control access to the barges once tied to the fleeting area by implementing TWIC as described in § 105.255 of this part.

* * * * *

Subpart D—Facility Security Plan (FSP)

■ 32. Revise § 105.405(a)(10) and (b) to read as follows:

§ 105.405 Format and content of the Facility Security Plan (FSP).

(a) * * *

(10) Security measures for access control, including designated public access areas;

* * * * *

(b) The FSP must describe in detail how the requirements of subpart B of this part will be met. FSPs that have been approved by the Coast Guard prior to March 26, 2007, do not need to be amended to describe their TWIC procedures until the next regularly scheduled resubmission of the FSP.

PART 106—MARITIME SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

■ 33. The authority citation for part 106 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

■ 34. Amend § 106.110 by adding paragraphs (d) and (e) to read as follows:

§ 106.110 Compliance dates.

* * * * *

(d) Persons required to obtain a TWIC under this part may enroll beginning after the date set by the Coast Guard in a Notice to be published in the **Federal Register**. This notice will be directed to all facilities and vessels within a specific COTP zone.

(e) Facility owners or operators must be operating in accordance with the TWIC provisions in this part by the date set by the Coast Guard in a Notice to be published in the **Federal Register**. This Notice will be published at least 90 days before compliance must begin, and will be directed to all facilities within a specific Captain of the Port zone, based on whether enrollment has been completed in that zone. Unless an earlier compliance date is specified in this manner, all facility owner or operators will need to implement their TWIC provisions no later than September 25, 2008.

■ 35. Revise § 106.200(b) to read as follows:

§ 106.200 Owner or operator.

* * * * *

(b) For each OCS facility, the OCS facility owner or operator must:

(1) Define the security organizational structure for each OCS facility and provide each person exercising security duties or responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS facility and identify how those officers can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the OCS facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including:

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the secure area are permitted to escort; and

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted.

(7) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(8) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required by the FSP for the new MARSEC Level;

(9) Ensure all breaches of security and security incidents are reported in accordance with part 101 of this subchapter;

(10) Ensure consistency between security requirements and safety requirements;

(11) Inform OCS facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(12) Ensure that protocols consistent with § 106.260(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and not yet received a TWIC, are in place; and

(13) If applicable, ensure that protocols consistent with § 106.262 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

■ 36. Amend § 106.205 by adding paragraphs (a)(4), (c)(13) and (d)(13) to read as follows:

§ 106.205 Company Security Officer (CSO).

(a) * * *

(4) The CSO must maintain a TWIC.

* * * * *

(c) * * *

(13) Knowledge of TWIC requirements.

(d) * * *

(13) Ensure the TWIC program is being properly implemented.

■ 37. Amend § 106.210 by adding paragraphs (a)(4) and (c)(15) to read as follows:

§ 106.210 OCS Facility Security Officer (FSO).

(a) * * *

(4) The FSO must maintain a TWIC.

* * * * *

(c) * * *

(15) Ensure the TWIC program is properly implemented.

■ 38. Amend § 106.215 by revising the introductory paragraph and redesignating paragraphs (k) and (l) as (l) and (m), respectively, and adding new paragraph (k) to read as follows:

§ 106.215 Company of OCS facility personnel with security duties.

Company and OCS facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(k) Familiarity with all relevant aspects of the TWIC program and how to carry them out;

* * * * *

■ 39. Amend § 106.220 by adding paragraph (f) to read as follows:

§ 106.220 Security training for all other OCS personnel.

* * * * *

(f) Familiarity with all relevant aspects of the TWIC program and how to carry them out.

■ 40. Revise § 106.260 to read as follows:

§ 106.260 Security measures for access control.

(a) *General.* The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board;

(3) Control access to the OCS facility; and

(4) Prevent an unescorted individual from entering the OCS facility unless the individual holds a duly issued TWIC and is authorized to be on the OCS facility.

(b) The OCS facility owner or operator must ensure that the following are specified:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access, including those points where TWIC access control procedures will be applied;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and the means by which they will be allowed access to the OCS facility; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The OCS facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with § 101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than seven consecutive calendar days if:

(i) The individual has reported the TWIC as lost, damaged or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of § 101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside of a secure area.

(4) With the exception of persons granted access according to paragraph (c)(2) of this section, all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.

(d) If the OCS facility owner or operator uses a separate identification system, ensure that it is coordinated with identification and TWIC systems in place on vessels conducting operations with the OCS facility.

(e) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) *MARSEC Level 1.* The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section.

(2) Screen persons and personal effects going aboard the OCS facility for dangerous substances and devices at the rate specified in the approved FSP;

(3) Conspicuously post signs that describe security measures currently in effect and clearly stating that:

(i) Boarding an OCS facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(4) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors and ensure that non-TWIC holders are denied unescorted access to the OCS facility;

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the OCS facility;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which OCS facility personnel and visitors have access;

(9) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(10) Provide a designated secure area on board, or in liaison with a vessel interfacing with the OCS facility, for

conducting inspections and screening of people and their personal effects; and

(11) Respond to the presence of unauthorized persons on board.

(g) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

(2) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

(3) Limiting the number of access points to the OCS facility by closing and securing some access points; or

(4) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

(h) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. The additional security measures may include:

(1) Screening all persons and personal effects for dangerous substances and devices;

(2) Being prepared to cooperate with responders;

(3) Limiting access to the OCS facility to a single, controlled access point;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending embarkation and/or disembarkation of personnel;

(6) Suspending the loading of stores or industrial supplies;

(7) Evacuating the OCS facility; or

(8) Preparing for a full or partial search of the OCS facility.

■ 41. Add § 106.262 to read as follows:

§ 106.262 Security measures for newly-hired employees.

(a) Newly-hired OCS facility employees may be granted entry to secure areas of the OCS facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the OCS facility. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired OCS facility employees may be granted the access provided for in paragraph (a) of this section if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The OCS facility owner or operator or Facility Security Officer (FSO) must have th enew hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The OCS facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport Web site (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment.

(3) The new hire presents an identification credential that meets the requirements of § 101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the OCS facility owner or operator or FSO have not been informed by the cognizant COTP that the individual poses a security threat; and

(5) There would be an adverse impact to OCS facility operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a Company Security Officer or FSO, or any individual being hired to perform OCS facility security duties.

(d) The new hire may not begin working at the OCS facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

■ 42. Revise § 106.405(b) to read as follows:

§ 106.405 Format and content of the Facility Security Plan (FSP).

* * * * *

(b) The FSP must describe in detail how the requirements of Subpart B of this part will be met. FSPs that have been approved by the Coast Guard prior to March 26, 2007 do not need to be amended to describe their TWIC procedures until the next regularly scheduled resubmission of the FSP.

PART 125—IDENTIFICATION CREDENTIALS FOR PERSONS REQUIRING ACCESS TO WATERFRONT FACILITIES OR VESSELS

■ 43. The authority citation for part 125 is revised to read as follows:

Authority: R.S. 4517, 4518, secs. 19, 2, 23 Stat. 58, 118, sec. 7, 49 Stat. 1936, sec. 1, 40 Stat. 220; 46 U.S.C. 570–572, 2, 689, and 70105; 50 U.S.C. 191, E.O. 10173, E.O. 10277, E.O. 10352, 3 CFR, 1949–1953 Comp. pp. 356, 778, 873.

■ 44. In § 125.09, revise paragraph (f) and add paragraph (g) to read as follows:

§ 125.09 Identification credentials.

* * * * *

(f) Transportation Worker Identification Credential.

(g) Such other identification as may be approved by the Commandant from time to time.

Title 46—Shipping

Chapter I—Coast Guard

PART 10—LICENSING OF MARITIME PERSONNEL

■ 45. The authority citation for part 10 continues to read as follows:

Authority: 14 U.S.C. 633; 31 U.S.C. 9701; 46 U.S.C. 2101, 2103, and 2110; 46 U.S.C. chapter 71; 46 U.S.C. 7502, 7505, 7701, and 8906; E.O. 10173; Department of Homeland Security Delegation No. 0170.1. sec. 11.107 is also issued under the authority of 44 U.S.C. 3507.

■ 46. Add new § 10.113 to read as follows:

§ 10.113 Transportation Worker Identification Credential.

By September 25, 2008 all mariners holding an active License, Certificate of Registry or STCW endorsement issued under this part must hold a valid Transportation Worker Identification Credential (TWIC) issued by the Transportation Security Administration under 49 CFR part 1572. Failure to obtain or hold a valid TWIC may serve as a basis for suspension or revocation of a mariner's license, COR or STCW endorsement under 46 U.S.C. 7702 and 7703.

PART 12—CERTIFICATION OF SEAMEN

■ 47. The authority citation for part 12 is revised to read as follows:

Authority: 31 U.S.C. 9701; 46 U.S.C. 2101, 2103, 2110, 7301, 7302, 7503, 7505, 7701, and 70105; Department of Homeland Security Delegation No. 0170.1.

■ 48. Add new § 12.01–11 to read as follows:

§ 12.01–11 Transportation Worker Identification Credential.

By September 25, 2008 all mariners holding a Merchant Mariner's Document or STCW endorsement issued under this part must hold a valid Transportation Worker Identification Credential (TWIC) issued by the Transportation Security Administration under 49 CFR part 1572. Failure to obtain or hold a valid TWIC may serve as a basis for suspension or revocation of a mariner's license, COR or STCW endorsement under 46 U.S.C. 7702 and 7703.

PART 15—MANNING REQUIREMENTS

■ 49. The authority citation for part 15 is revised to read as follows:

Authority: 46 U.S.C. 2101, 2103, 3306, 3703, 8101, 8102, 8104, 8105, 8301, 8304, 8502, 8503, 8701, 8702, 8901, 8902, 8903, 8904, 8905(b), 8906, 9102, and 70105; and Department of Homeland Security Delegation No. 0170.1.

■ 50. Add new § 15.415 to read as follows:

§ 15.415 Transportation Worker Identification Credential.

By September 25, 2008 a person may not employ or engage an individual, and an individual may not serve in a position in which an individual is required by law or regulation to hold an active License, Merchant Mariner Document (MMD), Certificate of Registry (COR), or STCW endorsement, unless the individual holds a valid Transportation Worker Identification Credential (TWIC). All mariners holding an active License, MMD, COR or STCW endorsement issued by the Coast Guard must hold a valid TWIC issued by the Transportation Security Administration under 49 CFR part 1572.

Title 49—Transportation

Chapter XII—Transportation Security Administration

Subchapter A—Administrative and Procedural Rules

■ 51. Add a new part 1515 to subchapter A to read as follows:

PART 1515—APPEAL AND WAIVER PROCEDURES FOR SECURITY THREAT ASSESSMENTS FOR INDIVIDUALS

Sec.
1515.1 Scope.
1515.3 Terms used in this part.
1515.5 Appeal of Initial Determination of Threat Assessment based on criminal conviction, immigration status, or mental capacity.
1515.7 Procedures for waiver of criminal offenses, immigration status, or mental capacity standards.
1515. 9 Appeal of security threat assessment based on other analyses.
1515.11 Review by administrative law judge and TSA Final Decision Maker.

Authority: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

§ 1515.1 Scope.

(a) *Appeal.* This part applies to applicants who are appealing an Initial Determination of Threat Assessment or an Initial Determination of Threat Assessment and Immediate Revocation in a security threat assessment as described in:

(1) 49 CFR part 1572 for a hazardous materials endorsement (HME) or a Transportation Worker Identification Credential (TWIC); or

(2) 49 CFR part 1540, Subpart C, for air cargo workers.

(b) *Waivers.* This part applies to applicants for an HME or TWIC who undergo a security threat assessment described in 49 CFR part 1572 and are eligible to request a waiver of certain standards.

§ 1515.3 Terms used in this part.

The terms used in 49 CFR parts 1500, 1540, 1570, and 1572 also apply in this part. In addition, the following terms are used in this part:

Administrative law judge means an administrative law judge appointed pursuant to the provisions of 5 U.S.C. 3105.

Applicant means an individual who has applied for one of the security threat assessments identified in 49 CFR 1515.1. This includes an individual who previously applied for and was found to meet the standards for the security threat assessment but TSA later determined that the individual poses a security threat.

Date of service means—

(1) In the case of personal service, the date of personal delivery to the residential address listed on the application;

(2) In the case of mailing with a certificate of service, the date shown on the certificate of service;

(3) In the case of mailing and there is no certificate of service, 10 days from the date mailed to the address designated on the application as the mailing address;

(4) In the case of mailing with no certificate of service or postmark, the date mailed to the address designated on the application as the mailing address shown by other evidence; or

(5) The date on which an electronic transmission occurs.

Day means calendar day.

Final Agency Order means an order issued by the TSA Final Decision Maker.

Decision denying a review of a waiver means a document issued by an administrative law judge denying a waiver requested under 49 CFR 1515.7.

Mail includes U.S. mail, or use of an express courier service.

Party means the applicant or the agency attorney.

Personal delivery includes hand-delivery or use of a contract or express messenger service, but does not include the use of Government interoffice mail service.

Properly addressed means a document that shows an address contained in agency records, a residential, business, or other address submitted by a person on any document provided under this subpart, or any other address shown by other reasonable and available means.

Substantial Evidence means such relevant evidence as a reasonable person might accept as adequate to support a conclusion.

Security threat assessment means the threat assessment for which the applicant has applied, as described in 49 CFR 1515.1.

TSA Final Decision Maker means the Administrator, acting in the capacity of the decision maker on appeal, or any person to whom the Administrator has delegated the Administrator's decision-making authority. As used in this subpart, the *TSA Final Decision Maker* is the official authorized to issue a final decision and order of the Administrator.

§ 1515.5 Appeal of Initial Determination of Threat Assessment based on criminal conviction, immigration status, or mental capacity.

(a) *Scope.* This section applies to applicants appealing from an Initial Determination of Threat Assessment that was based on one or more of the following:

(1) TSA has determined that an applicant for an HME or a TWIC has a disqualifying criminal offense described in 49 CFR 1572.103.

(2) TSA has determined that an applicant for an HME or a TWIC does

not meet the immigration status requirements as described in 49 CFR 1572.105.

(3) TSA has determined that an applicant for an HME or a TWIC is lacking mental capacity as described in 49 CFR 1572.109.

(b) *Grounds for appeal.* An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she meets the standards for the security threat assessment for which he or she is applying.

(1) *Initiating an appeal.* An applicant initiates an appeal by submitting a written reply to TSA, a written request for materials from TSA, or by requesting an extension of time in accordance with § 1515.5(f). If the applicant does not initiate an appeal within 60 days of receipt, the Initial Determination of Threat Assessment becomes a Final Determination of Threat Assessment.

(i) In the case of an HME, TSA also serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a mariner applying for TWIC, TSA also serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the appropriate Federal Maritime Security Coordinator (FMSC).

(2) *Request for materials.* Within 60 days of the date of service of the Initial Determination of Threat Assessment, the applicant may serve upon TSA a written request for copies of the materials upon which the Initial Determination was based.

(3) *TSA response.* (i) Within 60 days of receiving the applicant's request for materials, TSA serves the applicant with copies of the releasable materials upon the applicant on which the Initial Determination was based. TSA will not include any classified information or other protected information described in paragraph (f) of this section.

(ii) Within 60 days of receiving the applicant's request for materials or written reply, TSA may request additional information or documents from the applicant that TSA believes are necessary to make a Final Determination.

(4) *Correction of records.* If the Initial Determination of Threat Assessment was based on a record that the applicant believes is erroneous, the applicant may correct the record, as follows:

(i) The applicant contacts the jurisdiction or entity responsible for the information and attempts to correct or complete information contained in his or her record.

(ii) The applicant provides TSA with the revised record, or a certified true copy of the information from the appropriate entity, before TSA determines that the applicant meets the standards for the security threat assessment.

(5) *Reply.* (i) The applicant may serve upon TSA a written reply to the Initial Determination of Threat Assessment within 60 days of service of the Initial Determination, or 60 days after the date of service of TSA's response to the applicant's request for materials under paragraph (b)(1) of this section, if the applicant served such request. The reply must include the rationale and information on which the applicant disputes TSA's Initial Determination.

(ii) In an applicant's reply, TSA will consider only material that is relevant to whether the applicant meets the standards applicable for the security threat assessment for which the applicant is applying.

(6) *Final determination.* Within 60 days after TSA receives the applicant's reply, TSA serves a Final Determination of Threat Assessment or a Withdrawal of the Initial Determination as provided in paragraphs (c) or (d) of this section.

(c) *Final Determination of Threat Assessment.* (1) If the Assistant Administrator concludes that an HME or TWIC applicant does not meet the standards described in 49 CFR 1572.103, 1572.105, or 1572.109, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition—

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(2) The Final Determination includes a statement that the Assistant Administrator has reviewed the Initial Determination, the applicant's reply and any accompanying information, and any other materials or information available to him or her, and has determined that the applicant poses a security threat warranting denial of the security threat assessment for which the applicant has applied.

(d) *Withdrawal of Initial Determination.* If the Assistant Administrator or Assistant Secretary concludes that the applicant does not pose a security threat, TSA serves a Withdrawal of the Initial Determination upon the applicant, and the applicant's employer where applicable.

(e) *Nondisclosure of certain information.* In connection with the procedures under this section, TSA does not disclose classified information to the applicant, as defined in E.O. 12968 sec. 1.1(d), and reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

(f) *Extension of time.* TSA may grant an applicant an extension of time of the limits for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. TSA may grant itself an extension of time for good cause.

(h) *Judicial review.* For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order of the determination that the applicant does not meet the standards for a security threat assessment, in accordance with 49 U.S.C. 46110. The Final Determination is not a final TSA order to grant or deny a waiver, the procedures for which are in 49 CFR 1515.7 and 1515.11.

(i) *Appeal of immediate revocation.* If TSA directs an immediate revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (b) of this section. This applies—

(1) If TSA directs a State to revoke an HME pursuant to 49 CFR 1572.13(a).

(2) If TSA invalidates a TWIC by issuing an Initial Determination of Threat Assessment and Immediate Revocation pursuant to 49 CFR 1572.21(d)(3).

§ 1515.7 Procedures for waiver of criminal offenses, immigration status, or mental capacity standards.

(a) *Scope.* This section applies to the following applicants:

(i) An applicant for an HME or TWIC who has a disqualifying criminal offense described in 49 CFR 1572.103(a)(5) through (a)(12) or 1572.103(b) and who requests a waiver.

(ii) An applicant for an HME or TWIC who is an alien under temporary protected status as described in 49 CFR 1572.105 and who requests a waiver.

(iii) An applicant applying for an HME or TWIC who lacks mental capacity as described in 49 CFR 1572.109 and who requests a waiver.

(b) *Grounds for waiver.* TSA may issue a waiver of the standards described in paragraph (a) and grant an HME or TWIC if TSA determines that an applicant does not pose a security threat based on a review of information described in paragraph (c) of this section.

(c) *Initiating waiver.* (1) An applicant initiates a waiver as follows:

(i) Providing to TSA the information required in 49 CFR 1572.9 for an HME or 49 CFR 1572.17 for a TWIC.

(ii) Paying the fees required in 49 CFR 1572.405 for an HME or in 49 CFR 1572.501 for a TWIC.

(iii) Sending a written request to TSA for a waiver at any time, but not later than 60 days after the date of service of the Final Determination of Threat Assessment. The applicant may request a waiver during the application process, or may first pursue some or all of the appeal procedures in 49 CFR 1515.5 to assert that he or she does not have a disqualifying condition.

(2) In determining whether to grant a waiver, TSA will consider the following factors, as applicable to the disqualifying condition:

(i) The circumstances of the disqualifying act or offense.

(ii) Restitution made by the applicant.

(iii) Any Federal or State mitigation remedies.

(iv) Court records or official medical release documents indicating that the applicant no longer lacks mental capacity.

(v) Other factors that indicate the applicant does not pose a security threat warranting denial of the HME or TWIC.

(d) *Grant or denial of waivers.* (1) The Assistant Administrator will send a written decision granting or denying the waiver to the applicant within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(2) In the case of an HME, if the Assistant Administrator grants the waiver, the Assistant Administrator will send a Determination of No Security Threat to the licensing State within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(3) In the case of a mariner applying for a TWIC, if the Assistant Administrator grants the waiver, the Assistant Administrator will send a Determination of No Security Threat to the Coast Guard within 60 days of service of the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(4) If the Assistant Administrator denies the waiver the applicant may seek review in accordance with 49 CFR 1515.11. A denial of a waiver under this section does not constitute a final order of TSA as provided in 49 U.S.C. 46110.

(e) *Extension of time.* TSA may grant an applicant an extension of the time limits for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. TSA may grant itself an extension of time for good cause.

§ 1515.9 Appeal of security threat assessment based on other analyses.

(a) *Scope.* This section applies to an applicant appealing an Initial Determination of Threat Assessment as follows:

(1) TSA has determined that the applicant for an HME or TWIC poses a security threat as provided in 49 CFR 1572.107.

(2) TSA had determined that an air cargo worker poses a security threat as provided in 49 CFR 1540.205.

(b) *Grounds for appeal.* An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she does not pose a security threat. The appeal will be conducted in accordance with the procedures set forth in 49 CFR 1515.5(b), (e), and (f) and this section.

(c) *Final Determination of Threat Assessment.* (1) If the Assistant Administrator concludes that the applicant poses a security threat, following an appeal, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition—

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of an air cargo worker, TSA serves a Final Determination of Threat Assessment on the operator.

(2) The Final Determination includes a statement that the Assistant Administrator has reviewed the Initial Determination, the applicant's reply and any accompanying information, and any other materials or information available to him or her, and has determined that the applicant poses a security threat warranting denial of the security threat assessment for which the applicant has applied.

(d) *Withdrawal of Initial Determination.* If the Assistant Administrator concludes that the applicant does not pose a security threat, TSA serves a Withdrawal of the Initial Determination upon the applicant, and the applicant's employer where applicable.

(e) *Further review.* If the Assistant Administrator denies the appeal, the applicant may seek review in accordance with § 1515.11 of this part. A Final Determination issued under this section does not constitute a final order of TSA as provided in 49 U.S.C. 46110.

(f) *Appeal of immediate revocation.* If TSA directs an immediate revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (b) of this section. This applies—

(1) If TSA directs a State to revoke an HME pursuant to 49 CFR 1572.13(a).

(2) If TSA invalidates a TWIC by issuing an Initial Determination of Threat Assessment and Immediate Revocation pursuant to 49 CFR 1572.21(d)(3).

(3) If TSA withdraws a Determination of No Threat issued for an air cargo worker.

§ 1515.11 Review by administrative law judge and TSA Final Decision Maker.

(a) *Scope.* This section applies to the following applicants:

(1) An applicant who seeks review of a decision by TSA denying a request for a waiver under 49 CFR 1515.7.

(2) An applicant for an HME or a TWIC who has been issued a Final Determination of Threat Assessment on the grounds that he or she poses a security threat after an appeal as described in 49 CFR 1515.9.

(3) An air cargo worker who has been issued a Final Determination of Threat Assessment after an appeal as described in 49 CFR 1515.9.

(b) *Request for review.* No later than 30 calendar days from the date of service of the decision by TSA denying a waiver or of the Final Determination of Threat Assessment, the applicant may request a review. The review will be conducted by an administrative law judge who possesses the appropriate security clearance necessary to review classified or otherwise protected information and evidence. If the applicant fails to seek review within 30 calendar days, the Final Determination of Threat Assessment will be final with respect to the parties.

(1) The request for review must clearly state the issue(s) to be considered by the administrative law judge (ALJ), and include the following documents in support of the request:

(i) In the case of a review of a denial of waiver, a copy of the applicant's request for a waiver under 49 CFR 1515.7, including all materials provided by the applicant to TSA in support of the waiver request; and a copy of the decision issued by TSA denying the waiver request. The request for review may not include evidence or information that was not presented to TSA in the appeal under § 1515.9. The ALJ may consider only evidence or

information that was presented to TSA in the appeal. If the applicant has new evidence or information, the applicant must file a new appeal under § 1515.9 and the pending request for review of the Final Determination will be dismissed.

(ii) In the case of a review of a Final Determination of Threat Assessment, a copy of the Initial Notification of Threat Assessment and Final Notification of Threat Assessment; and a copy of the applicant's appeal under 49 CFR 1515.9, including all materials provided by the applicant to TSA in support of the appeal. The request for review may not include evidence or information that was not presented to TSA in the appeal under § 1515.9. The ALJ may consider only evidence or information that was presented to TSA in the appeal. If the applicant has new evidence or information, the applicant must file a new appeal under § 1515.9 and the pending request for review of the Final Determination will be dismissed.

(2) The applicant may include in the request for review a request for an in-person hearing before the ALJ.

(3) The applicant must file the request for review with the ALJ Docketing Center, U.S. Coast Guard, 40 S. Gay Street, Room 412, Baltimore, Maryland 21202–4022, ATTN: Hearing Docket Clerk.

(c) *Extension of Time.* The ALJ may grant an extension of the time limits described in this section for good cause shown. A request for an extension of time must be in writing and be received by the ALJ within a reasonable time before the due date to be extended; or an applicant may request an extension after the expiration of a due date by sending a written request describing why the failure to file within the time limits was excusable. This paragraph does not apply to time limits set by the administrative law judge during the hearing.

(d) *Duties of the Administrative Law Judge.* The ALJ may:

(1) Receive information and evidence presented to TSA in the request for a waiver under 49 CFR 1515.7 or an appeal under 49 CFR 1515.9.

(2) Consider the following criteria to determine whether a request for an in-person hearing is warranted:

(i) The credibility of evidence or information submitted in the applicant's request for a waiver; and

(ii) Whether TSA's waiver denial was made in accordance with the governing regulations codified at 49 CFR part 1515 and 49 CFR part 1572.

(3) Give notice of and hold conferences and hearings;

(4) Administer oaths and affirmations;

(5) Examine witnesses;

(6) Regulate the course of the hearing including granting extensions of time limits; and

(7) Dispose of procedural motions and requests, and issue a decision.

(e) *Hearing.* If the ALJ grants a request for a hearing, except for good cause shown, it will begin within 60 calendar days of the date of receipt of the request for hearing. The hearing is a limited discovery proceeding and is conducted as follows:

(1) If applicable and upon request, TSA will provide to the applicant requesting a review an unclassified summary of classified evidence upon which the denial of the waiver or Final Determination was based.

(i) TSA will not disclose to the applicant, or the applicant's counsel, classified information, as defined in E.O. 12968 section 1.1(d).

(ii) TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure by law or regulation.

(2) The applicant may present the case by oral testimony, documentary, or demonstrative evidence, submit rebuttal evidence, and conduct cross-examination, as permitted by the ALJ. Oral testimony is limited to the evidence or information that was presented to TSA in the request for a waiver or during the appeal. The Federal Rules of Evidence may serve as guidance, but are not binding.

(3) The ALJ will review any classified information on an ex parte, in camera basis, and may consider such information in rendering a decision if the information appears to be material and relevant.

(4) The standard of proof is substantial evidence on the record.

(5) The parties may submit proposed findings of fact and conclusions of law.

(6) If the applicant fails to appear, the ALJ may issue a default judgment.

(7) A verbatim transcript will be made of the hearing and will be provided upon request at the expense of the requesting party. In cases in which classified or otherwise protected evidence is received, the transcript may require redaction of the classified or otherwise protected information.

(8) The hearing will be held at TSA's Headquarters building or, on request of a party, at an alternate location selected by the administrative law judge for good cause shown.

(f) *Decision of the Administrative Law Judge.* (1) The record is closed once the certified transcript and all documents and materials have been submitted for the record.

(2) The ALJ issues an unclassified written decision to the applicant no later than 30 calendar days from the close of the record and serves the decision on the parties. The ALJ may issue a classified decision to TSA.

(3) The ALJ's decision may be appealed by either party to the TSA Final Decision Maker in accordance with paragraph (g).

(i) In the case of review of a waiver denial, unless appealed to the TSA Final Decision Maker, if the ALJ upholds the denial of the applicant's request for waiver, TSA will issue a Final Order Denying a Waiver to the applicant.

(ii) In the case of review of a waiver denial, unless appealed to the TSA Final Decision Maker, if the ALJ reverses the denial of the applicant's request for waiver, TSA will issue a Final Order granting a waiver to the applicant; and

(A) In the case of an HME, send a Determination of No Security Threat to the licensing State.

(B) In the case applicant for a TWIC, send a Determination of No Security Threat to the Coast Guard.

(C) In the case of an air cargo worker, send a Determination of No Security Threat to the operator.

(iii) In the case of review of an appeal under 49 CFR 1515.9, unless appealed to the TSA Final Decision Maker, if the ALJ determines that the applicant poses a security threat, TSA will issue a Final Order of Threat Assessment to the applicant.

(iv) In the case of review of an appeal under 49 CFR 1515.9, unless appealed to the TSA Final Decision Maker, if the ALJ determines that the applicant does not pose a security threat, TSA will issue a Withdrawal of the Final Determination to the applicant, and to the applicant's employer where applicable.

(g) *Review by the TSA Final Decision Maker.* (1) Either party may request that the TSA Final Decision Maker review the ALJ's decision by serving the request no later than 30 calendar days after the date of service of the decision of the ALJ.

(i) The request must be in writing, served on the other party, and may only address whether the decision is supported by substantial evidence on the record.

(ii) No later than 30 calendar days after receipt of the request, the other party may file a response.

(2) The ALJ will provide the TSA Final Decision Maker with a certified transcript of the hearing and all unclassified documents and material submitted for the record. TSA will

provide any classified materials previously submitted.

(3) No later than 60 calendar days after receipt of the request, or if the other party files a response, 30 calendar days after receipt of the response, or such longer period as may be required, the TSA Final Decision Maker issues an unclassified decision and serves the decision on the parties. The TSA Final Decision Maker may issue a classified opinion to TSA, if applicable. The decision of the TSA Final Decision Maker is a final agency order.

(i) In the case of review of a waiver denial, if the TSA Final Decision Maker upholds the denial of the applicant's request for waiver, TSA issues a Final Order Denying a Waiver to the applicant.

(ii) In the case of review of a waiver denial, if the TSA Final Decision Maker reverses the denial of the applicant's request for waiver, TSA will grant the waiver; and

(A) In the case of an HME, send a Determination of No Security Threat to the applicant and to the licensing State.

(B) In the case of a TWIC, send a Determination of No Security Threat to the applicant and to the Coast Guard.

(C) In the case of an air cargo worker, send a Determination of No Security Threat to the applicant and the operator.

(iii) In the case of review of an appeal under 49 CFR 1515.9, if the TSA Final Decision Maker determines that the applicant poses a security threat, TSA will issue a Final Order of Threat Assessment to the applicant.

(iv) In the case of review of an appeal under 49 CFR 1515.9, if the TSA Final Decision Maker determines that the applicant does not pose a security threat, TSA will issue a Withdrawal of the Final Determination to the applicant, and to the applicant's employer where applicable.

(h) *Judicial Review of a Final Order Denying a Waiver.* A person may seek judicial review of a final order of the TSA Final Decision Maker as provided in 49 U.S.C. 46110.

■ 52. Revise subpart C, part 1540 to read as follows:

Subpart C—Security Threat Assessments

Sec.
1540.201 Applicability and terms used in this subpart.
1540.203 Operator responsibilities.
1540.205 Procedures for security threat assessment.
1540.207 [Reserved]
1540.209 Security threat assessment fee.

Subpart C—Security Threat Assessments

§ 1540.201 Applicability and terms used in this subpart.

(a) This subpart includes the procedures that certain aircraft operators, foreign air carriers, and indirect air carriers must use to have security threat assessments done on certain individuals pursuant to 49 CFR 1544.228, 1546.213, 1548.7, 1548.15, and 1548.16. This subpart applies to the following:

(1) Each aircraft operator operating under a full program or full all-cargo program described in 49 CFR 1544.101(a) or (h).

(2) Each foreign air carrier operating under a program described in 49 CFR 1546.101(a), (b), or (e).

(3) Each indirect air carrier operating under a security program described in 49 CFR part 1548.

(4) Each individual with, or applying for, unescorted access to cargo under one of the programs described in (a)(1) through (a)(3) of this section.

(5) Each proprietor, general partner, officer, director, or owner of an indirect air carrier as described in 49 CFR 1548.16.

(b) For purposes of this subpart—

Applicant means the individuals listed in paragraph (a)(4) and (a)(5) of this section.

Operator means an aircraft operator, foreign air carrier, and indirect air carrier listed in paragraphs (a)(1) through (a)(3) of this section.

(c) An applicant poses a security threat under this subpart when TSA determines that he or she is known to pose or suspected of posing a threat—

(1) To national security;

(2) To transportation security; or

(3) Of terrorism.

§ 1540.203 Operator responsibilities.

(a) Each operator subject to this subpart must ensure that each applicant described in § 1540.201(a)(4) and (a)(5) completes the Security Threat Assessment described in this section.

(b) Each operator must:

(1) Authenticate the identity of the applicant by—

(i) Reviewing two forms of identification, one of which must be a government-issued picture identification; or

(ii) Other means approved by TSA.

(2) Submit to TSA a Security Threat Assessment application for each applicant that is signed by the applicant and that includes:

(i) Legal name, including first, middle, and last; any applicable suffix; and any other names used previously.

(ii) Current mailing address, including residential address if it differs from the current mailing address, and all other residential addresses for the previous five years, and e-mail address, if the individual has an e-mail address.

(iii) Date and place of birth.

(iv) Social security number (submission is voluntary, although failure to provide it may delay or prevent completion of the threat assessment).

(v) Gender.

(vi) Country of citizenship, and if naturalized in the United States, date of naturalization and certificate number.

(vii) Alien registration number, if applicable.

(viii) The following statement reading:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 49 U.S.C. 5103a. *Purpose:* This information is needed to verify your identity and to conduct a Security Threat Assessment to evaluate your suitability for completing the functions required by this position. Failure to furnish your SSN may result in delays in processing your application, but will not prevent completion of your Security Threat Assessment. Furnishing the other information is also voluntary; however, failure to provide it may delay or prevent the completion of your Security Threat Assessment, without which you may not be granted authorization to have unescorted access to air cargo subject to TSA security requirements. *Routine Uses:* Routine uses of this information include disclosure to TSA contractors or other agents who are providing services relating to the Security Threat Assessments; to appropriate governmental agencies for law enforcement or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement. For further information, please consult DHS/TSA 002 Transportation Security Threat Assessment System.

The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact, on this application can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of authorization or in the case of parties regulated under this section, removal of authorization to operate under this chapter, if applicable.

(3) Retain the applicant's signed Security Threat Assessment application, and any communications with TSA regarding the applicant's application, for 180 days following the end of the applicant's service to the operator.

(c) Records under this section may include electronic documents with electronic signature or other means of

personal authentication, where accepted by TSA.

§ 1540.205 Procedures for security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA conducts includes an intelligence-related check and a final disposition.

(b) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1540.203(b);

(2) Searches domestic and international Government databases to determine if an applicant meets the requirements of 49 CFR 1540.201(c) or to confirm an applicant's identity; and

(3) Adjudicates the results in accordance with 49 CFR 1540.201(c).

(c) *Final disposition.* Following completion of the procedures described in paragraph (b), the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant and the operator, if TSA determines that the applicant meets the security threat assessment standards in 49 CFR 1540.201(c).

(2) TSA serves an Initial Determination of Threat Assessment on the applicant and the operator, if TSA determines that the applicant does not meet the security threat assessment standards in 49 CFR 1540.201(c). The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.9; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of the Initial Determination of Threat Assessment in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) If the applicant does not appeal the Initial Determination of Threat Assessment, TSA serves a Final Determination of Threat Assessment on the operator and the applicant.

(e) *Withdrawal by TSA.* TSA serves a Withdrawal of the Initial Determination of Threat Assessment on the individual and a Determination of No Security Threat on the operator, if the appeal results in a determination that the individual does not pose a security threat.

§ 1540.207 [Reserved].

§ 1540.209 Security threat assessment fee.

(a) *Imposition of fees.* The fee of $28 is required for TSA to conduct a security threat assessment for an applicant.

(b) *Remittance of fees.* (1) The fee required under this subpart must be remitted to TSA, in a form and manner acceptable to TSA, each time the applicant or an aircraft operator, foreign air carrier, or indirect air carrier submits the information required under § 1540.203 to TSA.

(2) Fees remitted to TSA under this subpart must be payable to the ''Transportation Security Administration'' in U.S. currency and drawn on a U.S. bank.

(3) TSA will not issue any fee refunds, unless a fee was paid in error.

Subchapter D—Maritime and Land Transportation Security

■ 53. Revise part 1570 to read as follows:

PART 1570—GENERAL RULES

Sec.
1570.1 Scope.
1570.3 Terms used in this subchapter.
1570.5 Fraud and intentional falsification of records.
1570.7 Fraudulent use or manufacture; responsibilities of persons.
1570.9 Inspection of credential.
1570.11 Compliance, inspection, and enforcement.

Authority: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

§ 1570.1 Scope.

This part applies to any person involved in land or maritime transportation as specified in this subchapter.

§ 1570.3 Terms used in this subchapter.

For purposes of this subchapter:

Adjudicate means to make an administrative determination of whether an applicant meets the standards in this subchapter, based on the merits of the issues raised.

Alien means any person not a citizen or national of the United States.

Alien registration number means the number issued by the U.S. Department of Homeland Security to an individual when he or she becomes a lawful permanent resident of the United States or attains other lawful, non-citizen status.

Applicant means a person who has applied for one of the security threat assessments identified in this subchapter.

Assistant Administrator for Threat Assessment and Credentialing (Assistant Administrator) means the officer designated by the Assistant Secretary to administer the appeal and waiver programs described in this part, except where the Assistant Secretary is specifically designated in this part to administer the appeal or waiver program. The Assistant Administrator may appoint a designee to assume his or her duties.

Assistant Secretary means Assistant Secretary for Homeland Security, Transportation Security Administration (Assistant Secretary), the highest ranking TSA official, or his or her designee, and who is responsible for making the final determination on the appeal of an intelligence-related check under this part.

Commercial drivers license (CDL) is used as defined in 49 CFR 383.5.

Convicted means any plea of guilty or nolo contendere, or any finding of guilt, except when the finding of guilt is subsequently overturned on appeal, pardoned, or expunged. For purposes of this subchapter, a conviction is expunged when the conviction is removed from the individual's criminal history record and there are no legal disabilities or restrictions associated with the expunged conviction, other than the fact that the conviction may be used for sentencing purposes for subsequent convictions. In addition, where an individual is allowed to withdraw an original plea of guilty or nolo contendere and enter a plea of not guilty and the case is subsequently dismissed, the individual is no longer considered to have a conviction for purposes of this subchapter.

Determination of No Security Threat means an administrative determination by TSA that an individual does not pose a security threat warranting denial of an HME or a TWIC.

Federal Maritime Security Coordinator (FMSC) has the same meaning as defined in 46 U.S.C. 70103(a)(2)(G); is the Captain of the Port (COTP) exercising authority for the COTP zones described in 33 CFR part 3, and is the Port Facility Security Officer as described in the International Ship and Port Facility Security (ISPS) Code, part A.

Final Determination of Threat Assessment means a final administrative determination by TSA, including the resolution of related appeals, that an individual poses a security threat warranting denial of an HME or a TWIC.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, an indication of which must be on the individual's commercial driver's license, as provided in the Federal Motor Carrier Safety Administration (FMCSA) regulations in 49 CFR part 383.

Imprisoned or imprisonment means confined to a prison, jail, or institution for the criminally insane, on a full-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity. Time spent confined or restricted to a half-way house, treatment facility, or similar institution, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity, does not constitute imprisonment for purposes of this rule.

Incarceration means confined or otherwise restricted to a jail-type institution, half-way house, treatment facility, or another institution, on a full or part-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity.

Initial Determination of Threat Assessment means an initial administrative determination by TSA that an individual poses pose a security threat warranting denial of an HME or a TWIC.

Initial Determination of Threat Assessment and Immediate Revocation means an initial administrative determination that an individual poses a security threat that warrants immediate revocation of an HME or invalidation of a TWIC. In the case of an HME, the State must immediately revoke the HME if TSA issues an Initial Determination of Threat Assessment and Immediate Revocation. In the case of a TWIC, TSA invalidates the TWIC when TSA issues an Initial Determination of Threat Assessment and Immediate Revocation.

Invalidate means the action TSA takes to make a credential inoperative when it is reported as lost, stolen, damaged, no longer needed, or when TSA determines an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Lawful permanent resident means an alien lawfully admitted for permanent residence, as defined in 8 U.S.C. 1101(a)(20).

Maritime facility has the same meaning as ''facility'' together with ''OCS facility'' (Outer Continental Shelf facility), as defined in 33 CFR 101.105.

Mental health facility means a mental institution, mental hospital, sanitarium, psychiatric facility, and any other facility that provides diagnoses by licensed professionals of mental retardation or mental illness, including a psychiatric ward in a general hospital.

National of the United States means a citizen of the United States, or a person who, though not a citizen, owes permanent allegiance to the United States, as defined in 8 U.S.C. 1101(a)(22), and includes American Samoa and Swains Island.

Owner/operator with respect to a maritime facility or a vessel has the same meaning as defined in 33 CFR 101.105.

Revocation means the termination, deactivation, rescission, invalidation, cancellation, or withdrawal of the privileges and duties conferred by an HME or TWIC, when TSA determines an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Secure area means the area on board a vessel or at a facility or outer continental shelf facility, over which the owner/operator has implemented security measures for access control, as defined by a Coast Guard approved security plan. It does not include passenger access areas or public access areas, as those terms are defined in 33 CFR 104.106 and 105.106 respectively. Vessels operating under the waivers provided for at 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. Facilities subject to 33 CFR chapter I, subchapter H, part 105 may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure areas.

Security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

Sensitive security information (SSI) means information that is described in, and must be managed in accordance with, 49 CFR part 1520.

State means a State of the United States and the District of Columbia.

Transportation Worker Identification Credential (TWIC) means a Federal biometric credential, issued to an individual, when TSA determines that the individual does not pose a security threat.

Withdrawal of Initial Determination of Threat Assessment is the document that TSA issues after issuing an Initial Determination of Security Threat, when TSA determines that an individual does not pose a security threat that warrants denial of an HME or TWIC.

§ 1570.5 Fraud and intentional falsification of records.

No person may make, cause to be made, attempt, or cause to attempt any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with the subchapter, or exercise any privileges under this subchapter.

(b) Any reproduction or alteration, for fraudulent purpose, of any record, report, security program, access medium, or identification medium issued under this subchapter or pursuant to standards in this subchapter.

§ 1570.7 Fraudulent use or manufacture; responsibilities of persons.

(a) No person may use or attempt to use a credential, security threat assessment, access control medium, or identification medium issued or conducted under this subchapter that was issued or conducted for another person.

(b) No person may make, produce, use or attempt to use a false or fraudulently created access control medium, identification medium or security threat assessment issued or conducted under this subchapter.

(c) No person may tamper or interfere with, compromise, modify, attempt to circumvent, or circumvent TWIC access control procedures.

(d) No person may cause or attempt to cause another person to violate paragraphs (a)–(c) of this section.

§ 1570.9 Inspection of credential.

(a) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(b) Each person who has been issued or who possesses a TWIC must allow his or her TWIC to be read by a reader and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a PIN, to the reader, upon a request from TSA, the Coast Guard, other authorized DHS representative; or a Federal, State, or local law enforcement officer.

§ 1570.11 Compliance, inspection, and enforcement.

(a) Each owner/operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an owner/operator with—

(1) This subchapter and part 1520 of this chapter; and

(2) 46 U.S.C. 70105 and 49 U.S.C. 114.

(b) At the request of TSA, each owner/operator must provide evidence of compliance with this subchapter and part 1520 of this chapter, including copies of records.

■ 54. Revise part 1572 to read as follows:

PART 1572—CREDENTIALING AND SECURITY THREAT ASSESSMENTS

Subpart A—Procedures and General Standards

Sec.
1572.1 Applicability.
1572.3 Scope.
1572.5 Standards for security threat assessments.
1572.7 [Reserved]
1572.9 Applicant information required for HME security threat assessment.
1572.11 Applicant responsibilities for HME security threat assessment.
1572.13 State responsibilities for issuance of hazardous materials endorsement.
1572.15 Procedures for HME security threat assessment.
1572.17 Applicant information required for TWIC security threat assessment.
1572.19 Applicant responsibilities for a TWIC security threat assessment.
1572.21 Procedures for TWIC security threat assessment.
1572.23 TWIC expiration.
1572.24–1572.40 [Reserved]

Subpart B—Qualification Standards for Security Threat Assessments

1572.101 Scope.
1572.103 Disqualifying criminal offenses.
1572.105 Immigration status.
1572.107 Other analyses.
1572.109 Mental capacity.
1572.111–1572.139 [Reserved]

Subpart C—Transportation of Hazardous Materials From Canada or Mexico To and Within the United States by Land Modes

1572.201 Transportation of hazardous materials via commercial motor vehicle from Canada or Mexico to and within the United States.
1572.203 Transportation of explosives from Canada to the United States via railroad carrier.

Subpart D—[Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

1572.400 Scope and definitions.
1572.401 Fee collection options.
1572.403 Procedures for collection by States.
1572.405 Procedures for collection by TSA.

Subpart F—Fees for Security Threat Assessments for Transportation Worker Identification Credential (TWIC)

1572.500 Scope.
1572.501 Fee collection.

Authority: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

Subpart A—Procedures and General Standards

§ 1572.1 Applicability.

This part establishes regulations for credentialing and security threat assessments for certain maritime and land transportation workers.

§ 1572.3 Scope.

This part applies to—

(a) State agencies responsible for issuing a hazardous materials endorsement (HME); and

(b) An applicant who—

(1) Is qualified to hold a commercial driver's license under 49 CFR parts 383 and 384, and is applying to obtain, renew, or transfer an HME; or

(2) Is applying to obtain or renew a TWIC in accordance with 33 CFR parts 104 through 106 or 46 CFR part 10.

§ 1572.5 Standards for security threat assessments.

(a) *Standards.* TSA determines that an applicant poses a security threat warranting denial of an HME or TWIC, if—

(1) The applicant has a disqualifying criminal offense described in 49 CFR 1572.103;

(2) The applicant does not meet the immigration status requirements described in 49 CFR 1572.105;

(3) TSA conducts the analyses described in 49 CFR 1572.107 and determines that the applicant poses a security threat; or

(4) The applicant has been adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109.

(b) *Immediate Revocation/Invalidation.* TSA may invalidate a TWIC or direct a State to revoke an HME immediately, if TSA determines during the security threat assessment that an applicant poses an immediate threat to transportation security, national security, or of terrorism.

(c) *Violation of FMCSA Standards.* The regulations of the Federal Motor Carrier Safety Administration (FMCSA) provide that an applicant is disqualified from operating a commercial motor vehicle for specified periods, if he or she has an offense that is listed in the FMCSA rules at 49 CFR 383.51. If records indicate that an applicant has committed an offense that would disqualify the applicant from operating a commercial motor vehicle under 49 CFR 383.51, TSA will not issue a Determination of No Security Threat until the State or the FMCSA determine that the applicant is not disqualified under that section.

(d) *Waiver.* In accordance with the requirements of § 1515.7, applicants may apply for a waiver of certain security threat assessment standards.

(e) *Comparability of Other Security Threat Assessment Standards.* TSA may determine that security threat assessments conducted by other governmental agencies are comparable to the threat assessment described in this part, which TSA conducts for HME and TWIC applicants.

(1) In making a comparability determination, TSA will consider—

(i) The minimum standards used for the security threat assessment;

(ii) The frequency of the threat assessment;

(iii) The date of the most recent threat assessment; and

(iv) Whether the threat assessment includes biometric identification and a biometric credential.

(2) To apply for a comparability determination, the agency seeking the determination must contact the Assistant Program Manager, Attn: Federal Agency Comparability Check, Hazmat Threat Assessment Program, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202–4220.

(3) TSA will notify the public when a comparability determination is made.

(4) An applicant, who has completed a security threat assessment that is determined to be comparable under this section to the threat assessment described in this part, must complete the enrollment process and provide biometric information to obtain a TWIC, if the applicant seeks unescorted access to a secure area of a vessel or facility. The applicant must pay the fee listed in 49 CFR 1572.503 for information collection/credential issuance.

(5) TSA has determined that the security threat assessment for an HME under this part is comparable to the security threat assessment for TWIC.

(6) TSA has determined that the security threat assessment for a FAST card, under the Free and Secure Trade program administered by U.S. Customs and Border Protection, is comparable to the security threat assessment described in this part.

§ 1572.7 [Reserved].

§ 1572.9 Applicant information required for HME security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew an HME. When applying to transfer an HME from

one State to another, 49 CFR 1572.13(e) applies.

(a) Except as provided in (a)(12) through (16), the applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and e-mail address if available. If the applicant prefers to receive correspondence and notification via e-mail, the applicant should so state.

(3) Date of birth.

(4) Gender.

(5) Height, weight, hair color, and eye color.

(6) City, state, and country of birth.

(7) Immigration status and, if the applicant is a naturalized citizen of the United States, the date of naturalization.

(8) Alien registration number, if applicable.

(9) The State of application, CDL number, and type of HME(s) held.

(10) Name, telephone number, facsimile number, and address of the applicant's current employer(s), if the applicant's work for the employer(s) requires an HME. If the applicant's current employer is the U.S. military service, include branch of the service.

(11) Whether the applicant is applying to obtain, renew, or transfer an HME or for a waiver.

(12) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(13) Passport number. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(14) Department of State Consular Report of Birth Abroad. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(15) Whether the applicant has previously completed a TSA threat assessment, and if so the date and program for which it was completed. This information is voluntary and may expedite the adjudication process for applicants who have completed a TSA security threat assessment.

(16) Whether the applicant currently holds a federal security clearance, and if so, the date of and agency for which the clearance was performed. This information is voluntary and may expedite the adjudication process for applicants who have completed a federal security threat assessment.

(b) The applicant must provide a statement, signature, and date of signature that he or she—

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in 49 CFR 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application, or is applying for a waiver;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in 49 CFR 1572.103(b), during the five years before the date of the application, or is applying for a waiver;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103, or is applying for a waiver;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in 49 CFR 1572.103(a), in a civilian or military jurisdiction, or is applying for a waiver;

(5) Has not been adjudicated as lacking mental capacity or committed to a mental health facility involuntarily or is applying for a waiver;

(6) Meets the immigration status requirements described in 49 CFR 1572.105;

(7) Has or has not served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations, under 49 CFR 1572.11, impose a continuing obligation on the HME holder to disclose to the State if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. Purpose: This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a hazardous materials endorsement for a commercial driver's license. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. Routine Uses: Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(d) The applicant must certify and date receipt the following statement, immediately before the signature line:

The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application can be punished by fine or imprisonment or both (*See* section 1001 of Title 18 United States Code), and may be grounds for denial of a hazardous materials endorsement.

(e) The applicant must certify the following statement in writing:

I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified. If TSA or other law enforcement agency becomes aware of an imminent threat to a maritime facility or vessel, TSA may provide limited information necessary to reduce the risk of injury or damage to the facility or vessel.

§ 1572.11 Applicant responsibilities for HME security threat assessment.

(a) *Surrender of HME.* If an individual is disqualified from holding an HME under 49 CFR 1572.5(c), he or she must surrender the HME to the licensing State. Failure to surrender the HME to the State may result in immediate revocation under 49 CFR 1572.13(a) and/or civil penalties.

(b) *Continuing responsibilities.* An individual who holds an HME must surrender the HME as required in paragraph (a) of this section within 24 hours, if the individual—

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103; or

(2) Is adjudicated as lacking mental capacity, or committed to a mental health facility, as described in 49 CFR 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status, and/or is ordered removed from the United States.

(c) *Submission of fingerprints and information.* (1) An HME applicant must submit fingerprints and the information required in 49 CFR 1572.9, in a form acceptable to TSA, when so notified by the State, or when the applicant applies to obtain or renew an HME. The procedures outlined in 49 CFR 1572.13(e) apply to HME transfers.

(2) When submitting fingerprints and the information required in 49 CFR 1572.9, the fee described in 49 CFR 1572.503 must be remitted to TSA.

§ 1572.13 State responsibilities for issuance of hazardous materials endorsement.

Each State must revoke an individual's HME immediately, if TSA informs the State that the individual does not meet the standards for security threat assessment in 49 CFR 1572.5 and issues an Initial Determination of Threat Assessment and Immediate Revocation.

(a) No State may issue or renew an HME for a CDL, unless the State receives a Determination of No Security Threat from TSA.

(b) Each State must notify each individual holding an HME issued by that State that he or she will be subject to the security threat assessment described in this part as part of an application for renewal of the HME, at least 60 days prior to the expiration date of the individual's HME. The notice must inform the individual that he or she may initiate the security threat assessment required by this section at any time after receiving the notice, but no later than 60 days before the expiration date of the individual's HME.

(c) The State that issued an HME may extend the expiration date of the HME for 90 days, if TSA has not provided a Determination of No Security Threat or a Final Determination of Threat Assessment before the expiration date. Any additional extension must be approved in advance by TSA.

(d) Within 15 days of receipt of a Determination of No Security Threat or Final Determination of Threat Assessment from TSA, the State must—

(1) Update the applicant's permanent record to reflect:

(i) The results of the security threat assessment;

(ii) The issuance or denial of an HME; and

(iii) The new expiration date of the HME.

(2) Notify the Commercial Drivers License Information System (CDLIS) operator of the results of the security threat assessment.

(3) Revoke or deny the applicant's HME if TSA serves the State with a Final Determination of Threat Assessment.

(e) For applicants who apply to transfer an existing HME from one State to another, the second State will not require the applicant to undergo a new security threat assessment until the security threat assessment renewal period established in the preceding issuing State, not to exceed five years, expires.

(f) A State that is not using TSA's agent to conduct enrollment for the security threat assessment must retain the application and information required in 49 CFR 1572.9, for at least one year, in paper or electronic form.

§ 1572.15 Procedures for HME security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA completes includes a fingerprint-based criminal history records check (CHRC), an intelligence-related background check, and a final disposition.

(b) *Fingerprint-based check.* In order to conduct a fingerprint-based CHRC, the following procedures must be completed:

(1) The State notifies the applicant that he or she will be subject to the security threat assessment at least 60 days prior to the expiration of the applicant's HME, and that the applicant must begin the security threat assessment no later than 30 days before the date of the expiration of the HME.

(2) Where the State elects to collect fingerprints and applicant information, the State—

(i) Collects fingerprints and applicant information required in 49 CFR 1572.9;

(ii) Provides the applicant information to TSA electronically, unless otherwise authorized by TSA;

(iii) Transmits the fingerprints to the FBI/Criminal Justice Information Services (CJIS), in accordance with the FBI/CJIS fingerprint submission standards; and

(iv) Retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested.

(3) Where the State elects to have a TSA agent collect fingerprints and applicant information—

(i) TSA provides a copy of the signed application to the State;

(ii) The State retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested; and

(iii) TSA transmits the fingerprints to the FBI/CJIS, in accordance with the FBI/CJIS fingerprint submission standards.

(4) TSA receives the results from the FBI/CJIS and adjudicates the results of the check, in accordance with 49 CFR 1572.103 and, if applicable, 49 CFR 1572.107.

(c) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1572.9.

(2) Searches domestic and international Government databases described in 49 CFR 1572.105, 1572.107, and 1572.109.

(3) Adjudicates the results of the check in accordance with 49 CFR 1572.103, 1572.105, 1572.107, and 1572.109.

(d) *Final disposition.* Following completion of the procedures described in paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the State in which the applicant is authorized to hold an HME, if TSA determines that an applicant meets the security threat assessment standards described in 49 CFR 1572.5.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5 or 1515.9, as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer where appropriate, and the State, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5 and may pose an imminent threat to transportation or national security, or of terrorism. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of an HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5(h) or 1515.9(f), as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's

determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) If the applicant does not appeal the Initial Determination of Threat Assessment or Initial Determination of Threat Assessment and Immediate Revocation, TSA serves a Final Determination of Threat Assessment on the State in which the applicant applied for the HME, the applicant's employer where appropriate, and on the applicant, if the appeal of the Initial Determination results in a finding that the applicant poses a security threat.

(5) If the applicant appeals the Initial Determination of Threat Assessment or the Initial Determination of Threat Assessment and Immediate Revocation, the procedures in 49 CFR 1515.5 or 1515.9 apply.

(6) Applicants who do not meet certain standards in 49 CFR 1572.103, 1572.105, or 1572.109 may seek a waiver in accordance with 49 CFR 1515.7.

§ 1572.17 Applicant information required for TWIC security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew a TWIC.

(a) Except as provided in (a)(12) through (16), the applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and e-mail address if available. If the applicant wishes to receive notification that the TWIC is ready to be retrieved from the enrollment center via telephone rather than e-mail address, the applicant should state this and provide the correct telephone number.

(3) Date of birth.

(4) Gender.

(5) Height, weight, hair color, and eye color.

(6) City, state, and country of birth.

(7) Immigration status, and

(i) If the applicant is a naturalized citizen of the United States, the date of naturalization;

(ii) If the applicant is present in the United States based on a Visa, the type of Visa, the Visa number, and the date on which it expires; and

(iii) If the applicant is a commercial driver licensed in Canada and does not hold a FAST card, a Canadian passport.

(8) If not a national or citizen of the United States, the alien registration number and/or the number assigned to the applicant on the U.S. Customs and Border Protection Arrival-Departure Record, Form I–94.

(9) Except as described in paragraph (a)(9)(i) of this section, the reason that the applicant requires a TWIC, including, as applicable, the applicant's job description and the primary facility, vessel, or maritime port location(s) where the applicant will most likely require unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(i) Applicants who are commercial drivers licensed in Canada or Mexico who are applying for a TWIC in order to transport hazardous materials in accordance with 49 CFR 1572.201 and not to access secure areas of a facility or vessel, must explain this in response to the information requested in paragraph (a)(9) of this section.

(10) The name, telephone number, and address of the applicant's current employer(s), if working for the employer requires a TWIC. If the applicant's current employer is the U.S. military service, include the branch of the service. An applicant whose current employer does not require possession of a TWIC, does not have a single employer, or is self-employed, must provide the primary vessel or port location(s) where the applicant requires unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(11) If a credentialed mariner or applying to become a credentialed mariner, proof of citizenship as required in 46 CFR chapter I, subchapter B.

(12) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(13) Passport number, city of issuance, date of issuance, and date of expiration. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(14) Department of State Consular Report of Birth Abroad. This information is voluntary and may expedite the adjudication process for applicants who are U.S. citizens born abroad.

(15) Whether the applicant has previously completed a TSA threat assessment, and if so the date and program for which it was completed. This information is voluntary and may expedite the adjudication process for applicants who have completed a TSA security threat assessment.

(16) Whether the applicant currently holds a federal security clearance, and if so, the date of and agency for which the clearance was performed. This information is voluntary and may expedite the adjudication process for applicants who have completed a federal security threat assessment.

(b) The applicant must provide a statement, signature, and date of signature that he or she—

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in 49 CFR 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application, or is applying for a waiver;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in 49 CFR 1572.103(b), during the five years before the date of the application, or is applying for a waiver;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103, or is applying for a waiver;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in 49 CFR 1572.103(a), in a civilian or military jurisdiction, or is applying for a waiver;

(5) Has not been adjudicated as lacking mental capacity, or committed to a mental health facility involuntarily, or is applying for a waiver;

(6) Meets the immigration status requirements described in 49 CFR 1572.105;

(7) Has, or has not, served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations under 49 CFR 1572.19 impose a continuing obligation on the TWIC holder to disclose to TSA if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) Applicants, applying to obtain or renew a TWIC, must submit biometric information to be used for identity verification purposes. If an individual cannot provide the selected biometric, TSA will collect an alternative biometric identifier.

(d) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. Purpose: This information is needed to verify your identity

and to conduct a security threat assessment to evaluate your suitability for a Transportation Worker Identification Credential. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. Routine Uses: Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(e) The applicant must certify the following statement in writing:

As part of my employment duties, I am required to have unescorted access to secure areas of maritime facilities or vessels in which a Transportation Worker Identification Credential is required; I am now, or I am applying to be, a credentialed merchant mariner; or I am a commercial driver licensed in Canada or Mexico transporting hazardous materials in accordance with 49 CFR 1572.201.

(f) The applicant must certify and date receipt the following statement, immediately before the signature line:

The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application, can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of a Transportation Worker Identification Credential.

(g) The applicant must certify the following statement in writing:

I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified. If TSA or other law enforcement agency becomes aware of an imminent threat to a maritime facility or vessel, TSA may provide limited information necessary to reduce the risk of injury or damage to the facility or vessel.

§ 1572.19 Applicant responsibilities for a TWIC security threat assessment.

(a) *Implementation schedule.* Except as provided in paragraph (b) of this section, applicants must provide the information required in 49 CFR 1572.17, when so directed by the owner/operator.

(b) *Implementation schedule for certain mariners.* An applicant, who holds a Merchant Mariner Document (MMD) issued after February 3, 2003, and before the March 26, 2007, or a Merchant Marine License (License) issued after January 13, 2006, and before March 26, 2007, must submit the information required in this section, but is not required to undergo the security threat assessment described in this part.

(c) *Surrender of TWIC.* The TWIC is property of the Transportation Security Administration. If an individual is disqualified from holding a TWIC under 49 CFR 1572.5, he or she must surrender the TWIC to TSA. Failure to surrender the TWIC to TSA may result in immediate revocation under 49 CFR 1572.5(b) and/or civil penalties.

(d) *Continuing responsibilities.* An individual who holds a TWIC must surrender the TWIC, as required in paragraph (a) of this section, within 24 hours if the individual—

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in 49 CFR 1572.103; or

(2) Is adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status and/or is ordered removed from the United States.

(e) *Submission of fingerprints and information.* (1) TWIC applicants must submit fingerprints and the information required in 49 CFR 1572.17, in a form acceptable to TSA, to obtain or renew a TWIC.

(2) When submitting fingerprints and the information required in 49 CFR 1572.17, the fee required in 49 CFR 1572.503 must be remitted to TSA.

(f) *Lost, damaged, or stolen credentials.* If an individual's TWIC is damaged, or if a TWIC holder loses possession of his or her credential, he or she must notify TSA immediately.

§ 1572.21 Procedures for TWIC security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA conducts includes a fingerprint-based criminal history records check (CHRC), an intelligence-related check, and a final disposition.

(b) *Fingerprint-based check.* The following procedures must be completed to conduct a fingerprint-based CHRC:

(1) Consistent with the implementation schedule described in 49 CFR 1572.19(a) and (b), and as required in 33 CFR 104.200, 105.200, or 106.200, applicants are notified.

(2) During enrollment, TSA—

(i) Collects fingerprints, applicant information, and the fee required in 49 CFR 1572.17;

(ii) Transmits the fingerprints to the FBI/CJIS in accordance with the FBI/CJIS fingerprint submission standards.

(iii) Receives and adjudicates the results of the check from FBI/CJIS, in accordance with 49 CFR 1572.103 and, if applicable, 49 CFR 1572.107.

(c) *Intelligence-related check.* To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in 49 CFR 1572.17;

(2) Searches domestic and international Government databases required to determine if the applicant meets the requirements of 49 CFR 1572.105, 1572.107, and 1572.109;

(3) Adjudicates the results of the check in accordance with 49 CFR 1572.103, 1572.105, 1572.107, and 1572.109.

(d) *Final disposition.* Following completion of the procedures described in paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant if TSA determines that the applicant meets the security threat assessment standards described in 49 CFR 1572.5. In the case of a mariner, TSA also serves a Determination of No Security Threat on the Coast Guard.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the TWIC;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5 or 1515.9, as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer

where appropriate, the FMSC, and in the case of a mariner applying for a TWIC, on the Coast Guard, if TSA determines that the applicant does not meet the security threat assessment standards described in 49 CFR 1572.5 and may pose an imminent security threat. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of a TWIC and unescorted access to secure areas;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in 49 CFR 1515.5(h) or 1515.9(f), as applicable; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) If the applicant does not appeal the Initial Determination of Threat Assessment or Initial Determination of Threat Assessment and Immediate Revocation, TSA serves a Final Determination of Threat Assessment on the FMSC and in the case of a mariner, on the Coast Guard, and the applicant's employer where appropriate.

(5) If the applicant appeals the Initial Determination of Threat Assessment or the Initial Determination of Threat Assessment and Immediate Revocation, the procedures in 49 CFR 1515.5 or 1515.9 apply.

(6) Applicants who do not meet certain standards in 49 CFR 1572.103, 1572.105, or 1572.109 may seek a waiver in accordance with 49 CFR 1515.7.

§ 1572.23 TWIC expiration.

(a) A TWIC expires five years after the date it was issued at the end of the calendar day, except as follows:

(1) The TWIC was issued based on a determination that the applicant completed a comparable threat assessment. If issued pursuant to a comparable threat assessment, the TWIC expires five years from the date on the credential associated with the comparable threat assessment.

(2) The applicant is in a lawful nonimmigrant status category listed in 1572.105(a)(7), and the status expires, the employer terminates the employment relationship with the applicant, or the applicant otherwise ceases working for the employer. Under any of these circumstances, TSA deems the TWIC to have expired regardless of the expiration date on the face of the TWIC.

(b) TSA may issue a TWIC for a term less than five years to match the expiration of a visa.

§§ 1572.24—1572.40 [Reserved]

Subpart B—Standards for Security Threat Assessments

§ 1572.101 Scope.

This subpart applies to applicants who hold or are applying to obtain or renew an HME or TWIC, or transfer an HME. Applicants for an HME also are subject to safety requirements issued by the Federal Motor Carrier Safety Administration under 49 CFR part 383 and by the State issuing the HME, including additional immigration status and criminal history standards.

§ 1572.103 Disqualifying criminal offenses.

(a) *Permanent disqualifying criminal offenses.* An applicant has a permanent disqualifying offense if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following felonies:

(1) Espionage or conspiracy to commit espionage.

(2) Sedition, or conspiracy to commit sedition.

(3) Treason, or conspiracy to commit treason.

(4) A federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable State law, or conspiracy to commit such crime.

(5) A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101. A work stoppage, or other nonviolent employee-related action, resulting from an employer-employee dispute is not a transportation security incident.

(6) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a State law that is comparable.

(7) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).

(8) Murder.

(9) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.

(10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq, or a State law that is comparable, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph (a) of this section.

(11) Attempt to commit the crimes in paragraphs (a)(1) through (a)(4).

(12) Conspiracy or attempt to commit the crimes in paragraphs (a)(5) through (a)(10).

(b) *Interim disqualifying criminal offenses.* (1) The felonies listed in paragraphs (b)(2) of this section are disqualifying, if either:

(i) the applicant was convicted, or found not guilty by reason of insanity, of the crime in a civilian or military jurisdiction, within seven years of the date of the application; or

(ii) the applicant was incarcerated for that crime and released from incarceration within five years of the date of the TWIC application.

(2) The interim disqualifying felonies are:

(i) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.

(ii) Extortion.

(iii) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in paragraphs (a) or (b) of this section. Welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.

(iv) Bribery.

(v) Smuggling.

(vi) Immigration violations.

(vii) Distribution of, possession with intent to distribute, or importation of a controlled substance.

(viii) Arson.

(ix) Kidnapping or hostage taking.

(x) Rape or aggravated sexual abuse.

(xi) Assault with intent to kill.

(xi) Robbery.

(xii) Conspiracy or attempt to commit the crimes in this paragraph (b).

(xiii) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, *et seq.*, or a1036, or comparable State law that is comparable, other than the violations listed in paragraph (a)(10) of this section., for fraudulent entry into secure seaport areas.

(xiv) Conspiracy or attempt to commit the crimes in this paragraph (b).

(c) *Under want, warrant, or indictment.* An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in this section, is disqualified until the want or warrant is released or the indictment is dismissed.

(d) *Determination of arrest status.* (1) When a fingerprint-based check discloses an arrest for a disqualifying crime listed in this section without indicating a disposition, TSA will so notify the applicant and provide instructions on how the applicant must clear the disposition, in accordance with paragraph (d)(2) of this section.

(2) The applicant must provide TSA with written proof that the arrest did not result in conviction for the disqualifying criminal offense, within 60 days after the service date of the notification in paragraph (d)(1) of this section. If TSA does not receive proof in that time, TSA will notify the applicant that he or she is disqualified. In the case of an HME, TSA will notify the State that the applicant is disqualified, and in the case of a mariner applying for TWIC, TSA will notify the Coast Guard that the applicant is disqualified.

§ 1572.105 Immigration status.

(a) An individual applying for a security threat assessment for a TWIC or HME must be a national of the United States or—

(1) A lawful permanent resident of the United States;

(2) A refugee admitted under 8 U.S.C. 1157;

(3) An alien granted asylum under 8 U.S.C. 1158;

(4) An alien in valid M–1 nonimmigrant status who is enrolled in the United States Merchant Marine Academy or a comparable State maritime academy. Such individuals may serve as unlicensed mariners on a documented vessel, regardless of their nationality, under 46 U.S.C. 8103.

(5) A nonimmigrant alien admitted under the Compact of Free Association between the United States and the Federated States of Micronesia, the United States and the Republic of the Marshall Islands, or the United States and Palau.

(6) An alien in lawful nonimmigrant status who has unrestricted authorization to work in the United States, except—

(i) An alien in valid S–5 (informant of criminal organization information) lawful nonimmigrant status;

(ii) An alien in valid S–6 (informant of terrorism information) lawful nonimmigrant status;

(iii) An alien in valid K–1 (Fianco(e)) lawful nonimmigrant status; or

(iv) An alien in valid K–2 (Minor child of Fianco(e)) lawful nonimmigrant status.

(7) An alien in the following lawful nonimmigrant status who has restricted authorization to work in the United States—

(i) C–1/D Crewman Visa

(ii) H–1B Special Occupations;

(ii) H–1B1 Free Trade Agreement;

(iv) E–1 Treaty Trader;

(v) E–3 Australian in Specialty Occupation;

(vi) L–1 Intracompany Executive Transfer;

(vii) O–1 Extraordinary Ability; or

(viii) TN North American Free Trade Agreement.

(8) A commercial driver licensed in Canada or Mexico who is admitted to the United States under 8 CFR 214.2(b)(4)(i)(E) to conduct business in the United States.

(b) Upon expiration of a nonimmigrant status listed in paragraph (a)(7) of this section, an employer must retrieve the TWIC from the applicant and provide it to TSA.

(c) Upon expiration of a nonimmigrant status listed in paragraph (a)(7) of this section, an employee must surrender his or her TWIC to the employer.

(d) If an employer terminates an applicant working under a nonimmigrant status listed in paragraph (a)(7) of this section, or the applicant otherwise ceases working for the employer, the employer must notify TSA within 5 business days and provide the TWIC to TSA if possible.

(e) Any individual in removal proceedings or subject to an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC.

(f) To determine an applicant's immigration status, TSA will check relevant Federal databases and may perform other checks, including the validity of the applicant's alien registration number, social security number, or I–94 Arrival-Departure Form number.

§ 1572.107 Other analyses.

(a) TSA may determine that an applicant poses a security threat based on a search of the following databases:

(1) Interpol and other international databases, as appropriate.

(2) Terrorist watchlists and related databases.

(3) Any other databases relevant to determining whether an applicant poses, or is suspected of posing, a security threat, or that confirm an applicant's identity.

(b) TSA may also determine that an applicant poses a security threat, if the search conducted under this part reveals extensive foreign or domestic criminal convictions, a conviction for a serious crime not listed in 49 CFR 1572.103, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days.

§ 1572.109 Mental capacity.

(a) An applicant has mental incapacity, if he or she has been—

(1) Adjudicated as lacking mental capacity; or

(2) Committed to a mental health facility.

(b) An applicant is adjudicated as lacking mental capacity if—

(1) A court, board, commission, or other lawful authority has determined that the applicant, as a result of marked subnormal intelligence, mental illness, incompetence, condition, or disease, is a danger to himself or herself or to others, or lacks the mental capacity to conduct or manage his or her own affairs.

(2) This includes a finding of insanity by a court in a criminal case and a finding of incompetence to stand trial; or a finding of not guilty by reason of lack of mental responsibility, by any court, or pursuant to articles 50a and 76b of the Uniform Code of Military Justice (10 U.S.C. 850a and 876b).

(c) An applicant is committed to a mental health facility if he or she is formally committed to a mental health facility by a court, board, commission, or other lawful authority, including involuntary commitment and commitment for lacking mental capacity, mental illness, and drug use. This does not include commitment to a mental health facility for observation or voluntary admission to a mental health facility.

§§ 1572.111 through 1572.139 [Reserved]

Subpart C—Transportation of Hazardous Materials From Canada or Mexico To and Within the United States by Land Modes

§ 1572.201 Transportation of hazardous materials via commercial motor vehicle from Canada or Mexico to and within the United States.

(a) *Applicability.* This section applies to commercial motor vehicle drivers licensed by Canada and Mexico.

(b) *Terms used in this section.* The terms used in 49 CFR parts 1500, 1570, and 1572 also apply in this subpart. In addition, the following terms are used in this subpart for purposes of this section:

FAST means Free and Secure Trade program of the Bureau of Customs and Border Protection (CBP), a cooperative effort between CBP and the governments of Canada and Mexico to coordinate processes for the clearance of commercial shipments at the border.

Hazardous materials means material that has been designated as hazardous under 49 U.S.C. 5103 and is required to be placarded under subpart F of 49 CFR part 172 or any quantity of material that listed as a select agent or toxin in 42 CFR part 73.

(c) *Background check required.* A commercial motor vehicle driver who is licensed by Canada or Mexico may not transport hazardous materials into or within the United States unless the driver has undergone a background check similar to the one required of U.S.-licensed operators with a hazardous materials endorsement (HME) on a commercial driver's license, as prescribed in 49 CFR 1572.5.

(d) *FAST card.* A commercial motor vehicle driver who holds a current Free and Secure Trade (FAST) program card satisfies the requirements of this section. Commercial motor vehicle drivers who wish to apply for a FAST program card must contact the FAST Commercial Driver Program, Bureau of Customs and Border Protection (CBP), Department of Homeland Security.

(e) *TWIC.* A commercial motor vehicle driver who holds a TWIC satisfies the requirements of this section. Commercial vehicle drivers who wish to apply for a TWIC must comply with the rules in 49 CFR part 1572.

§ 1572.203 Transportation of explosives from Canada to the United States via railroad carrier.

(a) *Applicability.* This section applies to railroad carriers that carry explosives from Canada to the United States, using a train crew member who is not a U.S. citizen or lawful permanent resident alien of the United States.

(b) *Terms under this section.* For purposes of this section:

Customs and Border Protection (CBP) means the Bureau of Customs and Border Protection, an agency within the U.S. Department of Homeland Security.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known railroad carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known train crew member means an individual used to transport explosives from Canada to the United States, who has been determined by the Governments of Canada and the United States to present no known security concern.

Lawful permanent resident alien means an alien lawfully admitted for permanent residence, as defined by 8 U.S.C. 1101(a)(20).

Offeror means the person offering a shipment to the railroad carrier for transportation from Canada to the United States, and may also be known as the ''consignor'' in Canada.

Railroad carrier means ''railroad carrier'' as defined in 49 U.S.C. 20102.

(c) *Prior approval of railroad carrier, offeror, and train crew member.* (1) No railroad carrier may transport in commerce any explosive into the United States from Canada, via a train operated by a crew member who is not a U.S. national or lawful permanent resident alien, unless the railroad carrier, offeror, and train crew member are identified on a TSA list as a known railroad carrier, known offeror, and known train crew member, respectively.

(2) The railroad carrier must ensure that it, its offeror, and each of its crew members have been determined to be a known railroad carrier, known offeror, and known train crew member, respectively. If any has not been so determined, the railroad carrier must submit the following information to Transport Canada:

(i) The railroad carrier's identification, including—

(A) Official name;

(B) Business number;

(C) Any trade names; and

(D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

(A) Official name.

(B) Business number.

(C) Address.

(iii) The following information about any train crew member the railroad carrier may use to transport explosives into the United States from Canada, who is neither a U.S. national nor lawful permanent resident alien:

(A) Full name.

(B) Both current and most recent prior residential addresses.

(3) Transport Canada will determine whether the railroad carrier and offeror are legitimately doing business in Canada and will also determine whether the train crew members present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known railroad carriers, offerors, and train crew members and their identifying information.

(4) TSA will update and maintain the list of known railroad carriers, offerors, and train crew members and forward the list to CBP.

(5) Once included on the list, the railroad carriers, offerors, and train crew members need not obtain prior approval for future transport of explosives under this section.

(d) *TSA checks.* TSA may periodically check the data on the railroad carriers, offerors, and train crew members to confirm their continued eligibility, and may remove from the list any that TSA determines is not known or is a threat to security.

(e) *At the border.* (1) Train crew members who are not U.S. nationals or lawful permanent resident aliens. Upon arrival at a point designated by CBP for inspection of trains crossing into the United States, the train crew members of a train transporting explosives must provide sufficient identification to CBP to enable that agency to determine if each crew member is on the list of known train crew members maintained by TSA.

(2) *Train crew members who are U.S. nationals or lawful permanent resident aliens.* If CBP cannot verify that the crew member is on the list and the crew member is a U.S. national or lawful permanent resident alien, the crew

member may be cleared by CBP upon providing—

(i) A valid U.S. passport; or

(ii) One or more other document(s), including a form of U.S. Federal or state Government-issued identification with photograph, acceptable to CBP.

(3) *Compliance.* If a carrier attempts to enter the U.S. without having complied with this section, CBP will deny entry of the explosives and may take other appropriate action.

Subpart D—[Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

§ 1572.400 Scope and definitions.

(a) *Scope.* This part applies to—

(1) States that issue an HME for a commercial driver's license;

(2) Individuals who apply to obtain or renew an HME for a commercial driver's license and must undergo a security threat assessment under 49 CFR part 1572; and

(3) Entities who collect fees from such individuals on behalf of TSA.

(b) *Terms.* As used in this part:

Commercial driver's license (CDL) is used as defined in 49 CFR 383.5.

Day means calendar day.

FBI Fee means the fee required for the cost of the Federal Bureau of Investigation (FBI) to process fingerprint records.

Information Collection Fee means the fee required, in this part, for the cost of collecting and transmitting fingerprints and other applicant information under 49 CFR part 1572.

Threat Assessment Fee means the fee required, in this part, for the cost of TSA adjudicating security threat assessments, appeals, and waivers under 49 CFR part 1572.

TSA agent means an entity approved by TSA to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572, and fees in accordance with this part.

§ 1572.401 Fee collection options.

(a) *State collection and transmission.* If a State collects fingerprints and applicant information under 49 CFR part 1572, the State must collect and transmit to TSA the Threat Assessment Fee, in accordance with the requirements of 49 CFR 1572.403. The State also must collect and remit the FBI, in accordance with established procedures.

(b) *TSA agent collection and transmission.* If a TSA agent collects fingerprints and applicant information under 49 CFR part 1572, the agent must—

(1) Collect the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in accordance with procedures approved by TSA;

(2) Transmit to TSA the Threat Assessment Fee, in accordance with procedures approved by TSA; and

(3) Transmit to TSA the FBI Fee, in accordance with procedures approved by TSA and the FBI.

§ 1572.403 Procedures for collection by States.

This section describes the procedures that a State, which collects fingerprints and applicant information under 49 CFR part 1572; and the procedures an individual who applies to obtain or renew an HME, for a CDL in that State, must follow for collection and transmission of the Threat Assessment Fee and the FBI Fee.

(a) *Imposition of fees.* (1) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(2) The following FBI Fee is required for the FBI to process fingerprint identification records and name checks required under 49 CFR part 1572: the fee collected by the FBI under Pub. L. 101–515.

(3) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the State the Threat Assessment Fee and the FBI Fee, in a form and manner approved by TSA and the State, when the individual submits the application for the HME to the State.

(b) *Collection of fees.* (1) A State must collect the Threat Assessment Fee and FBI Fee, when an individual submits an application to the State to obtain or renew an HME.

(2) Once TSA receives an application from a State for a security threat assessment under 49 CFR part 1572, the State is liable for the Threat Assessment Fee.

(3) Nothing in this subpart prevents a State from collecting any other fees that a State may impose on an individual who applies to obtain or renew an HME.

(c) *Handling of fees.* (1) A State must safeguard all Threat Assessment Fees, from the time of collection until remittance to TSA.

(2) All Threat Assessment Fees are held in trust by a State for the beneficial interest of the United States in paying for the costs of conducting the security threat assessment, required by 49 U.S.C. 5103a and 49 CFR part 1572. A State holds neither legal nor equitable interest in the Threat Assessment Fees, except for the right to retain any accrued interest on the principal amounts collected pursuant to this section.

(3) A State must account for Threat Assessment Fees separately, but may commingle such fees with other sources of revenue.

(d) *Remittance of fees.* (1) TSA will generate and provide an invoice to a State on a monthly basis. The invoice will indicate the total fee dollars (number of applicants times the Threat Assessment Fee) that are due for the month.

(2) A State must remit to TSA full payment for the invoice, within 30 days after TSA sends the invoice.

(3) TSA accepts Threat Assessment Fees only from a State, not from an individual applicant for an HME.

(4) A State may retain any interest that accrues on the principal amounts collected between the date of collection and the date the Threat Assessment Fee is remitted to TSA, in accordance with paragraph (d)(2) of this section.

(5) A State may not retain any portion of the Threat Assessment Fee to offset the costs of collecting, handling, or remitting Threat Assessment Fees.

(6) Threat Assessment Fees, remitted to TSA by a State, must be in U.S. currency, drawn on a U.S. bank, and made payable to the ''Transportation Security Administration.''

(7) Threat Assessment Fees must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(8) TSA will not issue any refunds of Threat Assessment Fees.

(9) If a State does not remit the Threat Assessment Fees for any month, TSA may decline to process any HME applications from that State.

§ 1572.405 Procedures for collection by TSA.

This section describes the procedures that an individual, who applies to obtain or renew an HME for a CDL, must follow if a TSA agent collects and transmits the Information Collection Fee, Threat Assessment Fee, and FBI Fee.

(a) *Imposition of fees.* (1) The following Information Collection Fee is required for a TSA agent to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572: $38.

(2) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(3) The following FBI Fee is required for the FBI to process fingerprint identification records required under 49 CFR part 1572: The fee collected by the FBI under Pub. L. 101–515.

(4) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the TSA agent the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in a form and manner approved by TSA, when the individual submits the application required under 49 CFR part 1572.

(b) *Collection of fees.* A TSA agent will collect the fees required under this section, when an individual submits an application to the TSA agent, in accordance with 49 CFR part 1572.

(c) *Remittance of fees.* (1) Fees required under this section, which are remitted to a TSA agent, must be made in U.S. currency, drawn on a U.S. bank, and made payable to the ''Transportation Security Administration.''

(2) Fees required under this section must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(3) TSA will not issue any refunds of fees required under this section.

(4) Applications, submitted in accordance with 49 CFR part 1572, will be processed only upon receipt of all applicable fees under this section.

Subpart F—Fees for Security Threat Assessments for Transportation Worker Identification Credential (TWIC)

§ 1572.500 Scope.

(a) *Scope.* This part applies to—

(1) Individuals who apply to obtain or renew a Transportation Worker Identification Credential and must undergo a security threat assessment under 49 CFR part 1572; and

(2) Entities that collect fees from such individuals on behalf of TSA.

(b) *Terms.* As used in this part:

TSA agent means the entity approved by TSA to collect and transmit fingerprints and applicant information, and collect fees in accordance with this part.

§ 1572.501 Fee collection.

(a) *When fee must be paid.* When an applicant submits the information and fingerprints required under 49 CFR part 1572 to obtain or renew a TWIC, the fee must be remitted to TSA or its agent in accordance with the requirements of this section. Applications submitted in accordance with 49 CFR part 1572 will be processed only upon receipt of all required fees under this section.

(b) *Standard TWIC Fee.* The fee to obtain or renew a TWIC, other than for those identified in paragraph (a)(2) of this section, will be announced in the **Federal Register** after January 25, 2007. This fee is made up of the total of the following segments:

(1) The Enrollment Segment covers the cost for TSA or its agent to enroll applicants.

(2) The Full Card Production/Security Threat Assessment Segment covers the cost for TSA to conduct a security threat assessment.

(3) The FBI Segment covers the cost for the FBI to process fingerprint identification records under Pub. L. 101–515 and is $22. If the FBI amends this fee, TSA or its agent will collect the amended fee.

(c) *Reduced TWIC Fee.* The fee to obtain a TWIC when the applicant has undergone a comparable threat assessment in connection with an HME, a FAST card, other threat assessment deemed to be comparable under 49 CFR 1572.5(d), or holds an Merchant Mariner Document or Merchant Mariner License, will be announced in the **Federal Register** after January 25, 2007. This fee is made up of the following segments:

(1) The Enrollment Segment; and

(2) The Reduced Card Production/Security Threat Assessment Segment.

(d) *Card Replacement Fee.* The fee to replace a TWIC that has been lost, stolen, or damaged will be announced in the **Federal Register** after January 25, 2007.

(e) *Form of fee.* The TSA vendor will collect the fee required to obtain or renew a TWIC and will determine the method of acceptable payment, subject to approval by TSA.

(f) *Refunds.* TSA will not issue any refunds of fees required under this section.

(g) *Inflation adjustment.* The fees prescribed in this section, except the FBI fee, may be adjusted annually on or after October 1, 2007, by publication of an inflation adjustment. A final rule in the **Federal Register** will announce the inflation adjustment. The adjustment shall be a composite of the Federal civilian pay raise assumption and non-pay inflation factor for that fiscal year issued by the Office of Management and Budget for agency use in implementing OMB Circular A–76, weighted by the pay and non-pay proportions of total funding for that fiscal year. If Congress enacts a different Federal civilian pay raise percentage than the percentage issued by OMB for Circular A–76, the Department of Homeland Security may adjust the fees to reflect the enacted level. The required fee shall be the amount prescribed in paragraphs (a)(1)(i) and (a)(1)(ii), plus the latest inflation adjustment.

Dated: December 26, 2006.

Thad W. Allen,

Commandant, United States Coast Guard.

Dated: December 30, 2006.

Kip Hawley,

Assistant Secretary, Transportation Security Administration.

[FR Doc. 07–19 Filed 1–24–07; 8:45 am]

BILLING CODE 9110–05–P