## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

### 33 CFR Parts 101, 104, 105 and 106

**[Docket No. USCG–2007–28915]**

**RIN 1625–AB21**

## Transportation Worker Identification Credential (TWIC)—Reader Requirements

**AGENCY:** Coast Guard, DHS.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** In this Notice of Proposed Rulemaking (NPRM), the Coast Guard proposes to require owners and operators of certain vessels and facilities regulated by the Coast Guard to use electronic readers designed to work with the Transportation Worker Identification Credential (TWIC) as an access control measure. This NPRM also proposes additional requirements associated with electronic TWIC readers, including recordkeeping requirements for those owners and operators required to use an electronic TWIC reader, and security plan amendments to incorporate TWIC requirements. The TWIC program, including the proposed TWIC reader requirements in this rule, is an important component of the Coast Guard's multi-layered system of access control requirements and other measures designed to enhance maritime security.

This rulemaking action, once final, would build upon existing Coast Guard regulations designed to ensure that only individuals who hold a TWIC are granted unescorted access to secure areas at those locations. The Coast Guard has already promulgated regulations pursuant to the Maritime Transportation Security Act of 2002 (MTSA) that require mariners and other individuals to obtain a TWIC and present it for inspection by security personnel prior to gaining access to such secure areas. By requiring certain vessels and facilities to perform TWIC inspections using electronic TWIC readers, this rulemaking would further enhance security at those locations. This rulemaking would also implement the Security and Accountability For Every Port Act of 2006 electronic TWIC reader requirements.

**DATES:** Comments and related material must either be submitted to our online docket via *http://www.regulations.gov* on or before May 21, 2013 or reach the Docket Management Facility by that date. Comments sent to the Office of Management and Budget (OMB) on collection of information must reach OMB on or before May 21, 2013.

**ADDRESSES:** You may submit comments identified by Coast Guard docket number USCG–2007–28915 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

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

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

(3) *Fax:* 202–493–2251.

(4) *Delivery:* Room W12–140 on the Ground Floor of the West Building, 1200 New Jersey Avenue SE., Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

*Collection of Information Comments:* If you have comments on the collection of information discussed in this NPRM, you must also send comments to OMB's Office of Information and Regulatory Affairs (OIRA). To ensure that your comments to OIRA are received on time, the preferred methods are by email at *oira_submission@omb.eop.gov* (include the docket number and ''Attention: Desk Officer for Coast Guard, DHS'' in the subject line of the email) or fax at 202–395–6566. An alternate, though slower, method is by U.S. mail to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW., Washington, DC 20503, ATTN: Desk Officer, U.S. Coast Guard.

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this proposed rule, call Lieutenant Commander Loan T. O'Brien, Coast Guard, telephone 202–372–1133. If you have questions on viewing or submitting material to the docket, call Barbara Hairston, Program Manager, Docket Operations, telephone 202–366–9826.

**SUPPLEMENTARY INFORMATION:**

### Table of Acronyms

AHP Analytical Hierarchy Process
ANPRM Advanced Notice of Proposed Rulemaking
ASP Alternative Security Program
CAC Card Authentication Certificate
CCL Canceled Card List
CDC Certain Dangerous Cargoes
CFR Code of Federal Regulations
CGAA 2010 Coast Guard Authorization Act of 2010 (Pub. L. 111–281)
CHUID Card Holder Unique Identifier
CI/KR Critical Infrastructure/Key Resources
COTP Captain of the Port
DHS Department of Homeland Security
DPEA Draft Programmatic Environmental Assessment
FASC–N Federal Agency Smart Credential–Number
FONSI Finding of No Significant Impact
FSP Facility Security Plan
HSI Homeland Security Institute
ICE Test Initial Capability Evaluation Test
IPT Integrated Product Team
MARSEC Maritime Security
MERPAC Merchant Marine Personnel Advisory Committee
MISLE Marine Information for Safety and Law Enforcement
MODU Mobile Offshore Drilling Unit
MSRAM Maritime Security Risk Analysis Model
MTSA Maritime Transportation Security Act of 2002
NIST National Institute of Standards and Technology
NMSAC National Maritime Security Advisory Committee
NPRM Notice of Proposed Rulemaking
NTTAA National Technology Transfer and Advancement Act
NVIC Navigation and Vessel Inspection Circular
OCS Outer Continental Shelf
OIRA Office of Information and Regulatory Affairs
OMB Office of Management and Budget
OSV Offshore Supply Vessel
PAC–D Policy Advisory Council Decision
PACS Physical Access Control System
PIN Personal Identification Number
QTL Qualified Technology List
RUA Recurring Unescorted Access
SAFE Port Act Security and Accountability For Every Port Act of 2006
SBA Small Business Administration
SSI Sensitive Security Information
TSA Transportation Security Administration
TSAC Towing Safety Advisory Committee
TSI Transportation Security Incident
TWIC Transportation Worker Identification Credential
TWIC 1 Final Rule Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 72 FR 3492 (Jan. 25, 2007)
TWIC 1 NPRM Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Proposed Rules, 71 FR 29396 (May 22, 2006)
VSP Vessel Security Plan

### Table of Contents

## I. Public Participation and Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to *http://www.regulations.gov* and will include any personal information you have provided.

### *A. Submitting Comments*

If you submit a comment, please include the docket number for this rulemaking (USCG–2007–28915), indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation. You may submit your comments and material online, or by fax, mail, or hand delivery, but please use only one of these means. We recommend that you include your name and a mailing address, email address, or phone number in the body of your document so that we can contact you if we have any questions regarding your submission.

To submit your comment online, go to *http://www.regulations.gov* and use ''USCG–2007–28915'' as your search term. Locate this NPRM in the search results, click the corresponding ''Comment Now'' box, and follow the instructions. If you submit your comments by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit comments by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope.

We will consider all comments and material received during the comment period and may change this proposed rule based on your comments.

### *B. Viewing Comments and Documents*

To view comments, as well as documents mentioned in this preamble as being available in the docket, go to *http://www.regulations.gov,* and use ''USCG–2007–28915'' as your search term. The menu options on the left side of the Web page enable you to filter the results for public submissions and other types of documents. If you do not have access to the Internet, you may view the docket online by visiting the Docket Management Facility in Room W12–140 on the ground floor of the Department of Transportation West Building, 1200 New Jersey Avenue SE., Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. We have an agreement with the Department of Transportation to use the Docket Management Facility.

### *C. Privacy Act*

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

### *D. Public Meetings*

We intend to hold one or more public meetings regarding the proposals in this NPRM. A notice with the specific date and location of each meeting will be published in the **Federal Register** as soon as this information is known.

## II. Executive Summary

This section provides a concise description of the major proposals and policy decisions in this NPRM. We also provide a summary of the costs and benefits of this NPRM in this section.

### *A. Purpose of the Regulatory Action*

1. Need for the Regulatory Action

This regulatory action is necessary to improve the security of the nation's vessels and port facilities and to comply with statutory requirements. As authorized by the Maritime Transportation Security Act of 2002 [1] (MTSA), the Transportation Security Administration (TSA) established the TWIC program to address identity management shortcomings and vulnerabilities identified in the nation's transportation system and to comply

[1] Public Law 107–295, 116 Stat. 2064 (Nov. 2, 2002).

with the MTSA statutory requirements. On January 25, 2007, the Department of Homeland Security (DHS), through the Coast Guard and TSA, promulgated regulations that require mariners and other individuals granted unescorted access to secure areas of MTSA-regulated vessels or facilities to undergo a security threat assessment by TSA and obtain a TWIC.[2] This rulemaking, which would require owners and operators of certain types of vessels and facilities to use electronic TWIC readers, is necessary to advance the goals of the TWIC program. This rulemaking applies only to MTSA-regulated vessels and facilities. As described more fully below in this Executive Summary, we conducted a risk-based analysis of MTSA-regulated vessels and facilities to categorize them into one of three risk groups. Risk Group A is comprised of vessels and facilities that present the highest risk of being involved in a transportation security incident (TSI).[3] Vessels and facilities in Risk Group A would have new TWIC reader requirements under this rule. Vessels and facilities in Risk Groups B and C present progressively lower risks, and would continue to follow existing regulatory requirements for visual TWIC inspection.

The TWIC program, including the proposed TWIC reader requirements in this rule, is an important component of the Coast Guard's multi-layered system of access control requirements and other measures designed to enhance maritime security. Under this multi-layered system, owners and operators of MTSA-regulated vessels or facilities are required to submit for Coast Guard approval a comprehensive security plan detailing the access control and other security policies and procedures implemented on each vessel and facility. Security plans must identify and mitigate vulnerabilities. They accomplish this task by detailing the following items: (1) Security organization of the vessel or facility; (2) personnel training; (3) drills and exercises; (4) records and documentation; (5) response to changes in Maritime Security (MARSEC)[4] Level; (6) procedures for interfacing with other facilities and/or vessels; (7) Declarations of Security; (8) communications; (9) security systems and equipment maintenance; (10) security measures for access control; (11) security measures for restricted areas; (12) security measures for handling cargo; (13) security measures regarding vessel stores and bunkers; (14) security measures for monitoring; (15) security incident procedures; (16) audits and security plan amendments; (17) Security Assessment Reports and other security reports; and (18) TWIC procedures.[5] Coast Guard inspectors conduct routine and unannounced inspections and spot-checks to ensure proper implementation of approved security plans. The multi-layered security system also includes measures that consider broader security issues at U.S. ports and waterways, the coastal zone, the open ocean, and foreign ports.

The TWIC program's initial requirement on mariners and other individuals to obtain a TWIC provides security benefits in the maritime sector. Prior to this requirement, mariners and other individuals could access secure areas of MTSA-regulated vessels and facilities after presenting any number of identification cards, such as State-issued driver's licenses, mariner credentials, passports, and union identification cards. To detect invalid credentials, it was necessary for security personnel to become familiar with the appearance and security features of every type of acceptable credential. Moreover, since some government-issued credentials are used for purposes other than security, applicants for those credentials do not necessarily submit biographic and biometric information and undergo a security threat assessment or criminal background check. For example, a State-issued driver's license is a generally accepted form of government-issued identification in many places because it: (1) Is laminated or otherwise secure against tampering; (2) bears the individual's name and photograph; and (3) bears the name of the issuing authority. Nonetheless, while issuance of a driver's license is conditioned upon the applicant's successful completion of a course on driving instruction, road test, written test, eye examination, and other criteria specific to driving a motor vehicle, the applicant is not necessarily fingerprinted and screened against law enforcement databases for felony criminal activity or terrorist group affiliation. These are inherent shortcomings of an access control system that would permit access based on a patchwork of generic credentials issued to individuals who have undergone no security screening as a precondition to obtaining those credentials. In contrast, issuance of a TWIC is specifically conditioned on these security-related criteria.

Since April 15, 2009, TWIC has been the single credential used throughout the maritime sector. Accordingly, security personnel only need to become familiar with the appearance and security features of one credential. Moreover, unlike other government-issued credentials, TWIC is specifically designed for maritime transportation security. TWIC's purpose is to promote a vetted maritime workforce by establishing security-related eligibility criteria, and by requiring each TWIC-holder to undergo TSA's security threat assessment as part of the process of applying for and obtaining a TWIC.

While the existing security benefits of the TWIC program are substantial, electronic TWIC readers would provide greater security benefits because the TWIC card is designed to contain several enhanced security features that can only be utilized through the use of an electronic TWIC reader. One of these features is the set of two fingerprint templates from two different fingers embedded in each TWIC card. The Coast Guard is proposing to require the use of electronic TWIC readers, which would match the TWIC-holder's fingerprint to one of the embedded fingerprint templates. An electronic TWIC reader would provide a more reliable form of identity verification than the current visual comparison of the TWIC-holder's face to the photograph on the TWIC. Because a TWIC reader, when properly functioning, engages the security features of the card and cross-references with TSA's Canceled Card List (CCL), which the owner or operator would be required to update at least weekly, it is also more reliable than visual inspection for ensuring that a TWIC is not counterfeit or expired, or has not been reported lost, stolen, damaged, or revoked. When TWIC readers or TWICs are damaged or malfunctioning, the proposed rule would permit owners and operators to revert to visual inspection of the TWICs for 7 days if certain conditions are met.

Despite the enhanced reliability that TWIC readers would offer, not all vessels and facilities face security risks that justify the costs and other burdens that would result from a universal TWIC

[2] Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 72 FR 3492 (Jan. 25, 2007).

[3] 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 (49 CFR 1572.103).

[4] ''MARSEC Level'' means the level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S. (33 CFR 101.105).

[5] *See* 33 CFR 104.405 and 33 CFR 105.405.

reader requirement for all vessels and facilities. Therefore, in this rulemaking, we are considering a phased approach to implementing TWIC reader requirements by proposing such requirements first for vessels and facilities where the risk of harm is expected to be the greatest. We will continue to analyze risk data on MTSA-regulated vessels and facilities and consider whether additional or modified TWIC reader requirements are warranted in future rulemakings.

This Notice of Proposed Rulemaking (NPRM) proposes TWIC reader requirements for MTSA-regulated vessels and facilities that we have determined to present a heightened risk of being involved in a TSI, as described more fully below in Section III.C., ''Risk-Based Approach to Categorizing Vessels and Facilities.'' The Coast Guard assembled a panel of maritime security subject matter experts from the Coast Guard and TSA to conduct a risk-based analysis of MTSA-regulated vessels and facilities. The panel assessed the distinct types of vessels and facilities using three factors: (1) Maximum consequences to that vessel or facility resulting from a terrorist attack; (2) criticality to the nation's health, economy, and national security; and (3) utility of the TWIC in reducing risk.

For the first factor (maximum consequence resulting from a terrorist attack), we used the Coast Guard's Maritime Security Risk Analysis Model (MSRAM). MSRAM is a terrorism risk-analysis tool the Coast Guard uses to perform risk analysis on Critical Infrastructure and Key Resources (CI/KR) in the maritime domain, given a range of terrorist attack scenarios. The purpose of MSRAM is to capture and rank the security risks facing different types of potential terrorist targets spanning all CI/KR sectors in the nation's ports and on its waterways.

An initial step in the MSRAM process is to calculate the maximum potential consequence resulting from the total loss of a target, factoring in injury and loss of life, economic and environmental impact, symbolic effect, and national security impact. MSRAM then assesses risk for a range of scenarios (each involving a combination of potential terrorist target and method of attack) in terms of threat, vulnerability, and consequence. MSRAM considers the response capability of the owner or operator, local first responders, and Federal agencies to mitigate the consequences of an attack. MSRAM also considers input from Area Maritime Security Committees (AMSCs).[6]

For the second factor (criticality to the nation's health, economy, and national security), we considered the impact of the total loss of a vessel or facility beyond the immediate local consequences, taking into account the regional or national impacts on human health, the economy, and national security.

For the third factor (TWIC utility), we considered the utility of the TWIC program in reducing a vessel's or facility's vulnerability to a terrorist attack.

We combined the above three factors and developed an overall risk ranking of vessels and facilities by type. The panel then assigned numerical valued weights to the three factors. In determining the final weights, the panel chose the approach that best reflected its understanding of the maritime environment and TWIC program implementation, the importance of consequences in representing target attractiveness to terrorists, and the panel's expert perspective of risk. The actual numerical valued weights finalized by the panel are Sensitive Security Information (SSI). Finally, the panel calculated the priority scores for each vessel and facility type. At the end of this process, types of vessels and facilities with similar scores were combined into one of three risk groups.

Vessels and facilities that present a heightened risk for being involved in a TSI, Risk Group A, would have new TWIC reader requirements under this rule. For now, vessels and facilities that do not present this heightened risk would either continue to visually inspect TWICs or voluntarily deploy TWIC readers. We believe this approach would implement the TWIC reader program in a targeted manner that enhances the security of MTSA-regulated vessels and facilities without imposing undue burdens.

2. Legal Authority for the Regulatory Action

Under MTSA, the Secretary of Homeland Security (Secretary) is required to issue regulations designed to prevent individuals from entering secure areas of MTSA-regulated vessels or facilities without holding a TWIC or being accompanied by another individual holding a TWIC.[7] As a first step toward implementing that mandate, DHS, through the Coast Guard and TSA, promulgated a rule on January 27, 2007 that requires all maritime workers and other individuals to obtain a TWIC before they are granted unescorted access to secure areas in the maritime sector. We also required owners and operators of MTSA-regulated vessels or facilities to visually inspect the TWICs of individuals seeking access to secure areas at those locations. Additionally, we included alternatives to accommodate instances when an individual cannot present a TWIC because it has been lost, damaged, or stolen. In the January 27, 2007 rule, we did not implement TWIC reader requirements. Instead, we decided that TWIC reader requirements would follow in a separate rule after pilot testing TWIC readers in the maritime sector.

The Security and Accountability For Every (SAFE) Port Act of 2006[8] required the Secretary to conduct a pilot program to test the business processes, technology, and operational impacts of TWIC readers in the maritime environment, and to issue regulations that require the deployment of TWIC readers that are consistent with the findings of the pilot program.[9]

*B. Summary of the Major Provisions of the TWIC Reader Advanced Notice of Proposed Rulemaking and This NPRM*

On March 27, 2009, the Coast Guard published an advanced notice of proposed rulemaking on TWIC reader requirements (ANPRM).[10] The ANPRM proposed a risk-based approach to TWIC reader requirements. First, the ANPRM proposed to classify MTSA-regulated vessels and facilities into one of three risk groups, based on specific factors related to TSI consequence. Second, the ANPRM proposed TWIC reader requirements for vessels and facilities in the two highest risk groups (Risk Groups A and B). For the lowest risk group (Risk Group C), the ANPRM proposed visual TWIC inspection requirements instead of TWIC reader requirements because we determined that routine electronic biometric matching using TWIC readers would not be practical at lower risk vessels and facilities. This is consistent with the understanding that TWIC readers constitute one component

[6] AMSCs are committees established pursuant to 46 U.S.C. 70112(a)(2)(A). AMSCs are composed of at least seven members having an interest in the maritime security of a specific geographic area. AMSC members may be selected from government, public safety, law enforcement, maritime industry, and other port stakeholders. AMSCs assist in the development, review, and update of formal plans that detail maritime security measures and procedures for ports in a specific geographic area. *See* 33 CFR part 103.

[7] 46 U.S.C. 70105(a)–(f).

[8] Public Law 109–347, 120 Stat. 1884 (Oct. 13, 2006).

[9] 46 U.S.C. 70105(k)(3).

[10] Transportation Worker Identification Credential (TWIC)—Reader Requirements, 74 FR 13360 (March 27, 2009).

of a multi-layered maritime security system, but are not necessary or appropriate for every vessel or facility.

Based on the public comments received in response to the ANPRM, the findings of the DHS pilot program, and further analysis of the relevant issues, this NPRM reiterates many of the ANPRM's proposals, including retaining the ANPRM's risk-based framework for classifying vessels and facilities into the same three risk groups. As in the ANPRM, vessels and facilities are generally placed in higher risk groups based on the hazardous nature of the cargo handled or carried, or an increase in the number of passengers present. Our analysis demonstrates that it is necessary to maximize the use of the TWIC's security features where the risk is highest, as described more fully below in Section III.C., ''Risk-Based Approach to Categorizing Vessels and Facilities.'' We also believe it is necessary to carefully weigh the costs and benefits of TWIC reader requirements on the regulated population.

The main change in approach from the ANPRM to this NPRM is regarding the TWIC reader requirements for the different risk groups. Specifically, this NPRM proposes TWIC reader requirements for Risk Group A only. For Risk Groups B and C, this NPRM proposes to maintain the existing visual TWIC inspection requirements instead of TWIC reader requirements. This approach is designed to target the use of TWIC readers at the highest risk entities while minimizing the overall burden of the rule. Proposing TWIC reader requirements for Risk Group A only in this NPRM is indicative of our desire to minimize highest risks first, but should not be read to foreclose revised TWIC reader requirements in the future. We will continue to gather and analyze data to determine how the use of TWIC readers might be appropriate for each risk group. Any future changes will be made through rulemaking and the public will have an opportunity to comment.

This NPRM also proposes a requirement for owners and operators using TWIC readers to maintain records on each individual granted unescorted access to a secure area. Owners and operators would be required to maintain such records for a period of 2 years. Additionally, this NPRM proposes requirements to amend security plans to incorporate TWIC reader requirements for vessels and facilities in the highest risk group. These provisions are designed to ensure that owners and operators of vessels or facilities in Risk Group A comply with TWIC reader requirements.

TABLE ES–1—SUMMARY OF REQUIREMENTS/PROVISIONS PROPOSED IN THIS NPRM

| Proposed requirement or provision | Vessels (33 CFR part 104) | Facilities (33 CFR part 105) | OCS Facilities (33 CFR part 106) |
|---|---|---|---|
| Risk Group A classification | Vessels that carry CDC in bulk<br>Vessels certificated to carry more than 1,000 passengers.<br>Vessels towing one of the above | Facilities that handle CDC in bulk<br>Facilities that receive vessels certificated to carry more than 1,000 passengers.<br>Barge fleeting facilities that receive barges carrying CDC in bulk. | Not applicable. |
| Risk Group B classification | Vessels that carry hazardous materials other than CDC in bulk.<br>Vessels that carry flammable or combustible liquid cargoes.<br>Vessels certificated to carry 500–1,000 passengers.<br>Vessels towing one of the above. | Facilities that receive Risk Group B vessels. | All OCS facilities. |
| Risk Group C classification | Vessels that carry non-hazardous cargoes.<br>Vessels certificated to carry less than 500 passengers.<br>Vessels towing one of the above.<br>MODUs and OSVs. | Facilities that receive Risk Group C vessels. | Not applicable. |
| Movement between risk groups | Vessels are permitted to move between risk groups based on the materials carried at a given time. Described in VSP. | Facilities are permitted to move between risk groups based on the materials handled at a given time. Described in FSP. | Not applicable. |
| Visual TWIC inspection requirement. | Risk Groups B and C perform identity verification, card authentication, and card validation by visual TWIC inspection for each individual prior to being granted unescorted access to secure areas. | Risk Groups B and C perform identity verification, card authentication, and card validation by visual TWIC inspection for each individual prior to being granted unescorted access to secure areas. | Risk Groups B performs identity verification, card authentication, and card validation by visual TWIC inspection for each individual prior to being granted unescorted access to secure areas. |
| TWIC reader requirement | Risk Group A must use TWIC reader with biometric check for identity verification, card authentication, and card validation on each individual prior to being granted unescorted access to secure areas. | Risk Group A must use TWIC reader with biometric check for identity verification, card authentication, and card validation on each individual prior to being granted unescorted access to secure areas. | No requirement. |
| TWIC reader exemption based on minimum crew size. | Vessels with 14 or fewer TWIC-holding crew are exempt. | No exemption | Not applicable. |
| Physical placement of TWIC readers. | Vessel access points only | Access points to each secure area. | Not applicable. |

TABLE ES–1—SUMMARY OF REQUIREMENTS/PROVISIONS PROPOSED IN THIS NPRM—Continued

| Proposed requirement or provision | Vessels (33 CFR part 104) | Facilities (33 CFR part 105) | OCS Facilities (33 CFR part 106) |
|---|---|---|---|
| Unreadable fingerprints | Exception handling process may include PIN or alternate biometric. | Exception handling process may include PIN or alternate biometric. | Not applicable. |
| TWIC reader malfunction | Owner or operator performs visual TWIC inspection. Individuals that have been granted unescorted access with a valid TWIC in the past may still be granted such access for up to 7 days (with the possibility of an additional extension at the COTP's discretion). | Owner or operator performs visual TWIC inspection. Individuals that have been granted unescorted access with a valid TWIC in the past may still be granted such access for up to 7 days (with the possibility of an additional extension at the COTP's discretion). | Not applicable. |
| Recordkeeping | Records on each individual whose TWIC was scanned using a TWIC reader must be kept for 2 years. | Records on each individual whose TWIC was scanned using a TWIC reader must be kept for 2 years. | Not applicable. |
| Lost/stolen TWIC | Individuals following prescribed procedures may be granted unescorted access for no longer than 7 consecutive days. (Additional 30-day extension may be granted per Coast Guard guidance.). | Individuals following prescribed procedures may be granted unescorted access for no longer than 7 consecutive days. (Additional 30-day extension may be granted per Coast Guard guidance.). | Individuals following prescribed procedures may be granted unescorted access for no longer than 7 consecutive days. (Additional 30-day extension may be granted per Coast Guard guidance.) |
| Compliance deadline | 2 years after final rule publication | 2 years after final rule publication | Not applicable. Existing regulations apply. |

*C. Summary of Costs and Benefits*

Under MTSA, the Coast Guard regulates approximately 13,825 vessels, 3,270 facilities, and 56 Outer Continental Shelf (OCS) facilities. Of those MTSA-regulated facilities that could have potentially been regulated, 38 vessels and 532 facilities are affected by this proposed rule. We estimate the annualized cost of this proposed rule on the affected population of 38 vessels and 532 facilities to be about $26.5 million, while the 10-year cost is $186.1 million, discounted at 7 percent. The main cost drivers of this proposal are the acquisition, installation, and integration of TWIC readers into access control systems. Annual costs would be driven by costs associated with Canceled Card List updates, recordkeeping, training, system maintenance, and opportunity costs associated with failed TWIC reader transactions. We account for delays of up to two minutes for failed TWIC reader transactions. We estimate that 5% of TWIC-holders who access Risk Group A facilities and vessels will need to replace their TWICs annually, also contributing to the annual costs of this rule.

The benefits of this proposed rule include the enhancement of the security of vessels, ports, and other facilities by ensuring that only individuals who hold TWICs are granted unescorted access to secure areas at those locations. TWIC readers will not help identify valid cards that were obtained via fraudulent means, e.g., through unreported theft or the use of fraudulent IDs. Further, if the Coast Guard becomes aware of an imminent threat to a facility or vessel, the Coast Guard will notify the relevant Captain of the Port and other Federal, state, and local law enforcement officials and implement additional security measures as appropriate as a part of DHS's layered approach to security. This proposed rule would also implement the MTSA transportation security card requirement, as well as the SAFE Port Act of 2006 electronic TWIC reader requirements. The main benefit of this regulation, decreased terrorism risk, cannot be quantified given current data limitations.

TABLE ES–2—ESTIMATED COSTS AND FUNCTIONAL BENEFITS OF TWIC READER REQUIREMENTS [11]

| Category | NPRM |
|---|---|
| Applicability | High risk MTSA-regulated facilities and high risk MTSA-regulated vessels with greater than 14 crew. |
| Affected Population | 38 vessels.<br>532 facilities. |
| Costs ($ millions, 7% discount rate) | $26.5 (annualized).<br>$186.1 (10-year). |
| Costs (Qualitative) | Time to retrieve or replace lost PINs for use with TWIC cards. |
| Benefits (Qualitative) | Standardization of access control and credential verification throughout industry.<br>Enhanced access control and security at U.S. maritime facilities and onboard U.S. flagged vessels.<br>Reduction of human error when checking identification and manning access points. |

We used arisk-based approach to apply these regulatory requirements on less than 5 percent of the MTSA-regulated population, which represents approximately 80 percent of the potential consequences of a TSI. A discussion of our risk-based approach is provided below in Section III.C., ''Risk-Based Approach to Categorizing Vessels and Facilities.'' For a more detailed discussion of the methodology underpinning our risk-based approach, please refer to the Coast Guard report, ''Analysis of Transportation Worker Identification Credential (TWIC) Electronic Reader Requirements in the Maritime Sector,'' which is available for viewing in the public docket for this rulemaking. The proposals in this NPRM target the highest risk entities while minimizing the overall burden of the rule. Furthermore, we propose several types of relief in an effort to minimize the possible burden on the regulated population.

## III. Background and Purpose

This section provides a detailed discussion of the considerations and rationale for the policy decisions that informed this NPRM. The section that follows (Section IV.) sets forth the NPRM's proposals.

Section III.A. provides a general description of the TWIC and its security features, and also explains how the TWIC is used in the maritime sector as an access control measure.

Section III.B. discusses the statutory basis for this rulemaking, and summarizes the regulatory history of the TWIC program. The Coast Guard's most recent TWIC-related regulatory action is the ANPRM on TWIC reader requirements.

Section III.C. describes the ANPRM's risk-based approach for evaluating and categorizing types of vessels and facilities into risk groups. In doing so, this section summarizes the factors considered in developing the ANPRM's categorization system.

Section III.D. summarizes the ANPRM's proposals for TWIC reader requirements and other TWIC-related requirements for each risk group.

Section III.E. provides a detailed discussion of the public comments received during the ANPRM's comment period and public meeting. Section III.E. also provides our responses to those comments.

Sections III.F., III.G., III.H., and III.I. discuss DHS's TWIC Reader Pilot Program on TWIC reader functionality, the Homeland Security Institute's report on the ANPRM's risk group classification system, additional data sources, and Advisory Committee input in the rulemaking process, respectively.

### *A. General Information About the Transportation Worker Identification Credential*

This section provides a general description of the types of vessels and facilities currently covered under MTSA, the TWIC and its security features, and also explains how the TWIC is currently used in the maritime sector for access control.

Under MTSA, the Coast Guard is authorized to regulate vessels and facilities. For purposes of MTSA, the term ''facility'' means ''any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States.'' [12] For purposes of MTSA, the term ''vessel'' includes ''every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water.'' [13]

Coast Guard regulations implementing MTSA with respect to vessels [14] apply to: Mobile Offshore Drilling Units (MODUs), cargo vessels, or passenger vessels subject to International Convention for Safety of Life at Sea, 1974 (SOLAS), chapter XI–1 or Chapter XI–2; foreign cargo vessels greater than 100 gross register tons; generally, self-propelled U.S. cargo vessels greater than 100 gross tons; offshore supply vessels; vessels subject to the Coast Guard's regulations regarding passenger vessels; passenger vessels certificated to carry more than 150 passengers; passenger vessels carrying more than 12 passengers engaged on an international voyage; barges carrying, in bulk, cargoes regulated under the Coast Guard's regulations regarding tank vessels or Certain Dangerous Cargoes (CDCs); [15] barges carrying CDCs or cargo and miscellaneous vessels engaged on an international voyage; tankships; and generally, towing vessels greater than eight meters in register length engaged in towing barges.

Coast Guard regulations implementing MTSA with respect to facilities [16] apply to: Waterfront facilities handling dangerous cargoes (as generally defined in 49 CFR parts 170 through 179); waterfront facilities handling liquefied natural gas and liquefied hazardous gas; facilities transferring oil or hazardous materials in bulk; facilities that receive vessels certificated to carry more than 150 passengers; facilities that receive vessels subject to SOLAS, Chapter XI; facilities that receive foreign cargo vessels greater than 100 gross register tons; generally, facilities that receive U.S. cargo and miscellaneous vessels greater than 100 gross register tons; barge fleeting facilities that receive barges carrying, in bulk, cargoes regulated under the Coast Guard's regulations regarding tank vessels or CDCs; and fixed or floating facilities operating on the OCS for the purposes of engaging in the exploration, development, or production of oil, natural gas, or mineral resources (OCS facilities).

This rulemaking applies to the above-described vessels and facilities regulated by the Coast Guard pursuant to the authority granted in MTSA. The TWIC program is one component of the Coast Guard's multi-layered system of access control requirements and other measures designed to enhance maritime security. Under this multi-layered system, owners and operators of MTSA-regulated vessels or facilities are required to submit for Coast Guard approval a comprehensive security plan detailing the access control and other security policies and procedures implemented on each vessel and facility. Security plans must identify and mitigate vulnerabilities. They accomplish this task by detailing the following items: (1) Security organization of the vessel or facility; (2) personnel training; (3) drills and exercises; (4) records and documentation; (5) response to changes in Maritime Security (MARSEC) Level; (6) procedures for interfacing with other facilities and/or vessels; (7) Declarations of Security; (8) communications; (9) security systems and equipment maintenance; (10) security measures for access control; (11) security measures for restricted areas; (12) security measures for handling cargo; (13) security measures regarding vessel stores and bunkers; (14) security measures for monitoring; (15) security incident procedures; (16) audits and security plan amendments; (17) Security Assessment Reports and other security

[11] For a more detailed discussion of costs and benefits, see the full Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis available on the docket for this rulemaking. Appendix G of that document outlines the costs by provision and also discusses the complementary nature of the provisions and the subsequent difficulty in distinguishing independent benefits from individual provisions.

[12] 46 U.S.C. 70101(a)(2).

[13] 46 U.S.C. 115; 1 U.S.C. 3.

[14] *See* 33 CFR 104.105.

[15] The term ''Certain Dangerous Cargoes'' is defined in 33 CFR 101.105 by reference to 33 CFR 160.204, which lists all of the covered substances.

[16] *See* 33 CFR 105.105 and 106.105.

reports; and (18) TWIC procedures.[17] Coast Guard inspectors conduct routine and unannounced inspections and spot-checks to ensure proper implementation of approved security plans. The multi-layered security system also includes measures that consider broader security issues at U.S. ports and waterways, the coastal zone, the open ocean, and foreign ports.

The TWIC is a tamper-resistant biometric credential TSA issues to eligible maritime workers who require unescorted access to secure areas of MTSA-regulated vessels and facilities. To obtain a TWIC, applicants must provide biographic and biometric information and complete a TSA security threat assessment. Applicants are disqualified from obtaining a TWIC if their assessment reveals that they: have been convicted, or found not guilty by reason of insanity, of certain felonies; [18] are under want, warrant, or indictment for certain felonies; [19] have been released from incarceration within the preceding 5-year period for committing certain felonies; [20] may be denied admission to, or removed from, the United States under the Immigration and Nationality Act; [21] or otherwise pose a terrorism security risk to the United States.[22]

The face of the TWIC shows the holder's photograph, name, and TWIC expiration date, and the back shows a unique credential number (TWIC Serial Number). Because TWIC is the single credential used throughout the maritime sector, it provides considerable security benefits, including ensuring that individuals permitted to enter secure areas within the maritime transportation system have successfully undergone TSA's security threat assessment, involving a criminal history records check and an intelligence-related check. Before TWIC was in use, mariners and other individuals could access secure areas of MTSA-regulated vessels and facilities after presenting a State-issued driver's license or any number of other government-issued identification cards. To detect invalid credentials, it was necessary for security personnel to become familiar with the appearance and security features of every type of acceptable credential. Moreover, since some government-issued credentials are used for purposes other than security, applicants for those credentials do not necessarily submit biographic and biometric information and undergo a security threat assessment or criminal background check. For example, a State-issued driver's license is a generally accepted form of government-issued identification in many places because it: (1) Is laminated or otherwise secure against tampering; (2) bears the individual's name and photograph; and (3) bears the name of the issuing authority. Nonetheless, while issuance of a driver's license is conditioned upon the applicant's successful completion of a course on driving instruction, road test, written test, eye examination, and other criteria specific to driving a motor vehicle, the applicant is not necessarily fingerprinted and screened against law enforcement databases for felony criminal activity or terrorist group affiliation. These are inherent shortcomings of an access control system that would permit access based on a patchwork of generic credentials issued to individuals who have undergone no security screening as a precondition to obtaining those credentials. In contrast, issuance of a TWIC is specifically conditioned on these security-related criteria.

Since April 15, 2009, TWIC has been the single credential used throughout the maritime sector. Accordingly, security personnel only need to become familiar with the appearance and security features of one credential. Moreover, unlike other government-issued credentials, TWIC is specifically designed for transportation security. Its purpose is to ensure a vetted maritime workforce by establishing security-related eligibility criteria, and by requiring each TWIC-holder to undergo TSA's security threat assessment as part of the process of applying for and obtaining a TWIC.

In addition to its visible security features, the TWIC stores two electronically readable reference biometric templates (i.e., fingerprint templates), a personal identification number (PIN) selected by the TWIC-holder, a digital facial image, authentication certificates, and a Federal Agency Smart Credential-Number (FASC–N). These features enable the TWIC to be used in different ways for: (1) Identity verification; (2) card authentication; and (3) card validation.

Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. Identity can be verified by visually comparing the photo on the TWIC to the TWIC-holder. Using a TWIC reader, identity can be verified by matching one of the fingerprint templates stored in the TWIC to the TWIC-holder's live sample biometric, or by requiring the TWIC-holder to place the TWIC into a TWIC reader and enter a 6-, 7-, or 8-digit PIN selected by the TWIC-holder at the time of card activation.

Card authentication ensures that the TWIC is not counterfeit. Security personnel can authenticate a TWIC by visually inspecting the security features on the card. A TWIC reader authenticates the card by performing a challenge/response protocol using the Card Authentication Certificate (CAC) and the associated card authentication private key stored in the TWIC.[23]

Card validation using a TWIC reader ensures that the TWIC has not expired or been revoked by TSA, or reported as lost, stolen, or damaged. Security personnel can validate whether a TWIC has expired by visually checking the TWIC's expiration date. A TSA-canceled TWIC is placed on TSA's official Canceled Card List (CCL), which is updated daily.[24] Using a TWIC reader, card validity is confirmed by finding no match on the CCL and electronically checking the expiration date on the TWIC. Checks against the CCL may be performed electronically by downloading the list onto a TWIC reader or integrated Physical Access Control System (PACS).

*B. Statutory and Regulatory History*

This section discusses the statutory basis for this rulemaking, and summarizes the TWIC-related regulatory actions that precede this NPRM.

In the aftermath of the September 11, 2001 attacks, President George W. Bush signed Public Law 107–295, MTSA, 2002, which required the Secretary to publish rules that institute measures for the protection of U.S. maritime security as soon as practicable. On July 1, 2003, the Coast Guard published a series of six rules to promulgate maritime security requirements mandated by MTSA. These rules included the following ones: Implementation of National Maritime Security Initiatives (68 FR

[17] *See* 33 CFR 104.405 and 33 CFR 105.405.

[18] 46 U.S.C. 70105(c)(1)(A)–(B).

[19] 46 U.S.C. 70105(c)(1)(C).

[20] 46 U.S.C. 70105(c)(1)(D)(i).

[21] 46 U.S.C. 70105(c)(1)(D)(iii); 8 U.S.C. 1101 *et seq.*

[22] 46 U.S.C. 70105(c)(1)(D)(iv).

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

[24] TSA's Canceled Card List is available online at: *https://twicprogram.tsa.dhs.gov/TWICWebApp.*

39240); Area Maritime Security (68 FR 39284); Vessel Security (68 FR 39292); Facility Security (68 FR 39315); Outer Continental Shelf Facility Security (68 FR 39338); and Automatic Identification System (68 FR 39353). Most of these rules have been codified in 33 CFR subchapter H.

MTSA is the principal statutory authority for the TWIC program, and it requires the Secretary to issue regulations designed to prevent an individual from entering secure areas of MTSA-regulated vessels or facilities unless the individual holds a TWIC or is accompanied by another individual who holds a TWIC.[25]

On May 22, 2006, DHS, through the Coast Guard and TSA, published a notice of proposed rulemaking [26] (TWIC 1 NPRM) to implement the TWIC program in the maritime sector. On January 27, 2007, DHS, through the Coast Guard and TSA, issued a final rule [27] (TWIC 1 Final Rule) that required all credentialed merchant mariners and individuals granted unescorted access to secure areas of MTSA-regulated vessels or facilities to obtain a TWIC. Based on comments received in response to the TWIC 1 NPRM, and upon further analysis of the information available at the time, the Coast Guard concluded in the TWIC 1 Final Rule that it was premature to require the use of TWIC readers on vessels and at facilities.[28] The TWIC 1 Final Rule, however, stated that TWIC reader requirements would be addressed in a future rulemaking.[29] To date, TSA has issued approximately 2 million TWICs.[30] TWIC is now the single credential used throughout the maritime sector. For purposes of access control to MTSA-regulated vessels and facilities, security personnel only need to become familiar with the appearance and security features of one credential when determining whether to grant access to secure areas. Moreover, since the TWIC program is specifically designed for transportation security, it effectively ensures a vetted maritime workforce by establishing security-related eligibility criteria and by requiring each TWIC-holder to undergo TSA's security threat assessment as a precondition to obtaining a TWIC.

Section 104 of the SAFE Port Act of 2006 focused on how to further incorporate TWIC and TWIC readers into the MTSA security regime. Specifically, the SAFE Port Act supplemented various MTSA credentialing requirements by, among other things, requiring the Secretary to: (1) Conduct a TWIC reader testing pilot program (TWIC Pilot) to evaluate the business processes, technology, and operational impacts of a TWIC reader requirement; [31] and (2) promulgate final regulations requiring the use of TWIC readers in a manner consistent with the findings of the TWIC Pilot.[32]

While DHS collected data for the TWIC Pilot, the Coast Guard published the ANPRM on March 27, 2009, discussing the Coast Guard's preliminary thoughts on potential TWIC reader requirements, and opening a public dialog on how to best implement those requirements. The ANPRM proposed a framework that would separate individual MTSA-regulated vessels, MTSA-regulated facilities, and MTSA-regulated OCS facilities into one of three risk groups. Vessels and facilities are generally placed in higher risk groups based on the hazardous nature of the cargo handled or carried, or an increase in the number of passengers present. This framework is described more fully below in Section III.C., ''Risk-Based Approach to Categorizing Vessels and Facilities.'' The ANPRM proposed TWIC reader requirements for vessels and facilities in Risk Groups A and B, the two highest risk groups. For Risk Group C, the ANPRM proposed visual TWIC inspection requirements instead of TWIC reader requirements because we determined that the frequent electronic matching of a biometric would not be practical at lower risk vessels and facilities. This is consistent with the understanding that TWIC readers constitute one component of a multi-layered maritime security system, but are not necessary or appropriate for every vessel or facility.

Based on the public comments received in response to the ANPRM, the TWIC Pilot findings, and further analysis of the relevant issues, this NPRM reiterates many of the ANPRM's proposals, including retaining the ANPRM's risk-based framework for classifying vessels and facilities into the same three risk groups. Our analysis demonstrates that it is necessary to maximize the use of the TWIC's security features where the risk is highest, as described more fully below in Section III.C., ''Risk-Based Approach to Categorizing Vessels and Facilities.'' We also believe it is necessary to carefully weigh the costs and benefits of TWIC reader requirements on the regulated population.

The primary change in approach from the ANPRM to this NPRM is regarding the TWIC reader requirements for the different risk groups. Specifically, this NPRM proposes TWIC reader requirements for Risk Group A only. For Risk Groups B and C, this NPRM proposes to maintain the existing visual TWIC inspection requirements instead of TWIC reader requirements. This approach is designed to target the use of TWIC readers at the highest risk entities while minimizing the overall burden of the rule. Proposing TWIC reader requirements for Risk Group A only in this NPRM is indicative of our desire to minimize highest risks first, but should not be read to foreclose revised TWIC reader requirements in the future. We will continue to gather and analyze data to determine how the use of TWIC readers might be appropriate for each risk group. Any future changes will be made through rulemaking and the public will have an opportunity to comment.

The Coast Guard Authorization Act of 2010 (Pub. L. 111–281) (CGAA 2010) contains two provisions we refer to into this rulemaking. First, Section 809 of the CGAA 2010 authorizes the Secretary to exempt any credentialed mariner who is not granted unescorted access to secure areas of a vessel from the requirement to possess a TWIC. Second, Section 814 of the CGAA 2010 allows the Secretary to permit the use of alternate biometrics, such as a retina scan, to verify the identification of individuals using TWIC when the individual's fingerprints are not able to be taken or read.

### *C. Risk-Based Approach to Categorizing Vessels and Facilities*

This section describes the ANPRM's risk-based approach for evaluating and categorizing types of vessels and facilities into risk groups.

The Coast Guard assembled a panel of maritime security subject matter experts from the Coast Guard and TSA to conduct a risk-based analysis of MTSA-regulated vessels and facilities. The panel determined that the Analytical Hierarchy Process (AHP) would provide an effective basis for applying the panel's judgment to weigh and apply several key factors to the assessment of types of vessels and facilities. The AHP

[25] 46 U.S.C. 70105(a)–(f).

[26] Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 71 FR 29396 (May 22, 2006).

[27] Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 72 FR 3492 (Jan. 25, 2007).

[28] *See* 72 FR 3512.

[29] *See* 72 FR 3512.

[30] For statistics and other general information about the TWIC program, visit the TSA Web site at *http://www.tsa.gov/twic.*

[31] 46 U.S.C. 70105(k)(1).

[32] 46 U.S.C. 70105(k)(3).

is the core methodology in the Expert Choice [33] collaborative decision support tool, which was used in the Coast Guard's risk-based analysis. The AHP was originally developed in the 1970s by Dr. Thomas Saaty, then a professor at the Wharton School, University of Pennsylvania. The methodology has since gained wide acceptance and is used by Fortune 500 companies, Federal agencies, and MBA programs as a structured technique for achieving solutions to complex problems. Federal agencies that have used the AHP/Expert Choice include the National Institute of Standards and Technology, Department of the Army, Department of the Air Force, Bureau of Land Management, Bureau of Engraving and Printing, Department of Agriculture, Department of Energy, Department of Housing and Urban Development, Department of State, Defense Information Systems Agency, Department of Veterans Affairs, and the Federal Aviation Administration.

The AHP provides a comprehensive and rational framework for structuring a problem, representing and quantifying its elements, relating those elements to overall goals, and for evaluating a set of alternative solutions. The AHP has been used by government and industry to assess alternatives and arrive at solutions when faced problems that present disparate criteria and factors to consider.

The Coast Guard's panel of subject matter experts identified 68 distinct types of vessels and facilities based on their purpose or operational description. The panel then assessed each of the 68 types of vessels and facilities using three factors: (1) Maximum consequences to that vessel or facility resulting from a terrorist attack; (2) criticality to the nation's health, economy, and national security; and (3) utility of the TWIC in reducing risk.

For the first factor (maximum consequence resulting from a terrorist attack), we used the Coast Guard's Maritime Security Risk Analysis Model (MSRAM). MSRAM is a terrorism risk-analysis tool the Coast Guard uses to perform risk analysis on Critical Infrastructure and Key Resources (CI/KR) in the maritime domain, given a range of terrorist attack scenarios. The purpose of MSRAM is to capture and rank the security risks facing different types of potential terrorist targets (e.g., waterfront facilities, vessels, bridges, and other infrastructure) spanning all CI/KR sectors in the nation's ports and on its waterways.

An initial step in the MSRAM process is to calculate the maximum potential consequence resulting from the total loss of a target, factoring in injury and loss of life, economic and environmental impact, symbolic effect, and national security impact. MSRAM then assesses risk for a range of scenarios (each involving a combination of potential terrorist target and method of attack) in terms of threat, vulnerability, and consequence. MSRAM considers the response capability of the owner or operator, local first responders, and Federal agencies to mitigate the consequences of an attack. MSRAM also considers input from Area Maritime Security Committees (AMSCs).[34]

In consultation with representatives from AMSCs throughout the country, we have compiled MSRAM risk information from Coast Guard Sectors and Captains of the Port (COTPs) into a database that provides an overall national view of terrorism risk to maritime assets. For purposes of this proposed rule, we focused on MSRAM data specific to MTSA-regulated vessels and facilities, and used it to address the maximum consequence that would occur from the total loss of a vessel or facility caused by a TSI resulting from a terrorist attack. We averaged these MSRAM consequences across similar types of vessels and facilities to develop a standard risk for each type.

For the second factor (criticality to the nation's health, economy, and national security), we considered the impact of the total loss of a vessel or facility beyond the immediate local consequences, taking into account the regional or national impacts on human health, the economy, and national security.

For the third factor (TWIC utility), we considered the utility of the TWIC program in reducing a vessel or facility's vulnerability to a terrorist attack.

Using the AHP, we combined the above three factors and developed an overall risk ranking of vessels and facilities by type. As a first step in this process, the panel identified the 68 vessel and facility types, and the three criteria described above. As a second step, the panel considered different approaches to assigning numerical valued weights to the three factors. In determining the final weights, the panel chose the approach that best reflected its understanding of the maritime environment and TWIC program implementation, the importance of consequences in representing target attractiveness to terrorists, and the panel's expert perspective of risk. The actual numerical valued weights finalized by the panel are SSI. Finally, the panel used the AHP math in Expert Choice to calculate the priority scores for each vessel and facility type. At the end of this process, types of vessels and facilities with similar scores were combined into one of three risk groups. For a more detailed discussion of the panel's methodology, a copy of the panel's report, ''Analysis of Transportation Worker Identification Credential (TWIC) Electronic Reader Requirements in the Maritime Sector'' is available for viewing in the public docket for this rulemaking.

The ANPRM then proposed different TWIC-related requirements for each risk group. In determining the cutoff points between risk groups, risk rankings were graphed to identify natural breaks that occurred in the data. For vessels, these breaks generally occurred where there was a change in the hazardous nature of the cargo or where the number of passengers carried aboard a vessel increased. Similarly, for facilities, these breaks generally occurred where there was a change in the hazardous nature of the materials stored or handled at a facility, or where the number of passengers accessing a facility increased.

We engaged the Homeland Security Institute (HSI) to conduct an independent peer review of the risk-based analysis that formed the basis of the proposals in the ANPRM. HSI conducted its peer review in accordance with OMB Memorandum M–05–03, ''Issuance of OMB's 'Final Information Quality Bulletin for Peer Review''' (Dec. 16, 2004) [35] (OMB Review Guidelines). The OMB Review Guidelines establish government-wide guidance aimed at enhancing the practice of peer review of government science documents. Peer review is designed to increase the quality and credibility of the scientific information generated across the Federal government. The OMB Review Guidelines also discuss the concept of a ''highly influential scientific assessment,'' as one that would have at least one of the following characteristics: (1) Potential impact of

[33] Information about Expert Choice is available at *www.expertchoice.com.*

[34] AMSCs are committees established pursuant to 46 U.S.C. 70112(a)(2)(A). AMSCs are composed of at least seven members having an interest in the maritime security of a specific geographic area. AMSC members may be selected from government, public safety, law enforcement, maritime industry, and other port stakeholders. AMSCs assist in the development, review, and update of formal plans that detail maritime security measures and procedures for ports in a specific geographic area. *See* 33 CFR part 103.

[35] *OMB Memorandum M–05–03* is available for viewing at *http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-03.pdf.*

more than $500 million in any year; (2) novel, controversial, or precedent-setting; or (3) significant interagency interest. HSI advised that the TWIC program is, at a minimum, precedent-setting. Therefore, peer review of the Coast Guard's underlying analysis would be considered at the level of a ''highly influential scientific assessment.''

HSI conducted its peer review and issued a final report (HSI Report) on October 21, 2008. HSI independently reproduced the results based on the information provided in the Coast Guard report, ''Analysis of Transportation Worker Identification Credential (TWIC) Electronic Reader Requirements in the Maritime Sector,'' and deemed the process to be technically sound. The HSI report also acknowledged that ''no decision-aid tools * * * including the AHP, should be considered to lead to unassailable results.'' [36] A portion of the HSI Report is considered Sensitive Security Information (SSI) under 49 CFR Part 15. Therefore, a non-SSI version of the HSI Report is available for viewing in the public docket for this rulemaking. A summary of the HSI Report recommendations is provided below in Section III.G. ''HSI Report.''

*D. ANPRM Proposals*

This section provides a summary of the ANPRM's proposals for TWIC reader requirements and other TWIC-related requirements. Later parts of Section III. ''Background and Purpose'' discuss the public comments received on the ANPRM, as well our responses to those comments. For a more detailed discussion of the ANPRM's proposals, please refer to the ANPRM at 74 FR 13360. We retain many of the ANPRM's proposals in the NPRM. We delete or modify a number of the ANPRM's proposals in the NPRM. To avoid any confusion, if you wish to focus specifically on the proposals in the NPRM, please refer to Section IV. ''Section-by-Section Description of Proposed Rule.''

1. Classification of Vessels and Facilities Into Risk Groups

For vessels subject to 33 CFR part 104, the ANPRM proposed the following risk group classifications:

Risk Group A

(1) Vessels that carry Certain Dangerous Cargoes (CDC) in bulk;

(2) Vessels certificated to carry more than 1,000 passengers; and

(3) Towing vessels engaged in towing a barge or barges subject to paragraphs (1) or (2).

Risk Group B

(1) Vessels that carry hazardous materials other than CDC in bulk;

(2) Vessels subject to 46 CFR Chapter I, Subchapter D, that carry any flammable or combustible liquid cargoes or residues; [37]

(3) Vessels certificated to carry 500 to 1,000 passengers; and

(4) Towing vessels engaged in towing a barge or barges subject to paragraphs (1), (2), or (3).

Risk Group C

(1) Vessels carrying non-hazardous cargoes that are required to have a vessel security plan (VSP);

(2) Vessels certificated to carry less than 500 passengers;

(3) Towing vessels engaged in towing a barge or barges subject to paragraphs (1) or (2);

(4) Mobile Offshore Drilling Units (MODUs); and

(5) Offshore Supply Vessels (OSVs) subject to 46 CFR Chapter I, Subchapters L or I.

The risk group classifications in the ANPRM for facilities are similar to those for vessels. For facilities subject to 33 CFR part 105, the ANPRM proposed the following risk group classifications:

Risk Group A

(1) Facilities that handle CDC in bulk;

(2) Facilities that receive vessels certificated to carry more than 1,000 passengers; and

(3) Barge fleeting facilities that receive barges carrying CDC in bulk.

Risk Group B

(1) Facilities that receive vessels that carry hazardous materials other than CDC in bulk;

(2) Facilities that receive vessels subject to 46 CFR Chapter I, Subchapter D, that carry any flammable or combustible liquid cargoes or residues;

(3) Facilities that receive vessels certificated to carry 500 to 1,000 passengers; and

(4) Facilities that receive towing vessels engaged in towing a barge or barges carrying hazardous materials other than CDC in bulk, carrying crude oil, or towing vessels certificated to carry 500 to 1,000 passengers.

Risk Group C

(1) Facilities that receive vessels carrying non-hazardous cargoes that are required to have a VSP;

(2) Facilities that receive towing vessels engaged in towing a barge or barges carrying non-hazardous cargoes;

(3) Facilities that receive vessels certificated to carry less than 500 passengers.

The ANPRM proposed to classify all OCS facilities subject to 33 CFR part 106 into Risk Group B.

In the ANPRM, we contemplated the possibility that vessels and facilities may move from one risk group to another, based on the cargo handled or carried at any given time. In those instances, the owner or operator would be expected to explain, in an amended security plan, how their regulatory compliance program would change to reflect movement between risk groups, with particular attention to the security measures to be taken when moving from a lower risk group to a higher risk group.

2. TWIC Reader Requirements for Risk Group A

The ANPRM proposed TWIC reader requirements and other TWIC-related requirements for Risk Group A that would utilize the TWIC's most protective measures for identity verification, card authentication, and card validation.

For identity verification, owners and operators of vessels or facilities in Risk Group A would be required to either match the TWIC-holder's fingerprint to one of the fingerprint templates stored in the TWIC, or match the TWIC-holder's alternate biometric (e.g., retina scan, hand geometry, or other biometric) to one captured and stored in a PACS. A TWIC reader can work as a stand-alone unit, or it can be integrated into a facility's PACS. Either way, the owner or operator would be required to use a TWIC reader from the official list of TSA-approved TWIC readers. The biometric match would need to be made using a TWIC reader and/or PACS before the individual is granted unescorted access to secure areas.

When electronically matching biometrics within a PACS, an owner or operator would be permitted to use a different biometric than a fingerprint (e.g., an iris scan or hand geometry), stored in the PACS and matched to the biometric of the TWIC-holder. The owner or operator would be required to link their system to the TWIC in such a manner that the PACS precludes access to someone who does not have a TWIC, or to someone other than the

[36] *See* HSI Report, p. 2.

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

individual to whom the TWIC has been issued. This requirement means that the TWIC would need to be read and the stored biometric identifier matched against the TWIC-holder's fingerprint at least once, when the individual's information is entered into the PACS. Before relying on the alternate biometric, it must be verified, through a one-to-one fingerprint match, that the individual presenting the TWIC is actually the person to whom the TWIC was issued.

In the ANPRM, we recognized that while PIN verification could be used to enhance the accuracy of identity verification, this method presents operational and environmental challenges. The PIN can only be entered when the TWIC is inserted into a ''contact'' TWIC reader, where the TWIC is inserted into a slot allowing direct contact between the TWIC reader and the chip embedded in the TWIC. Comments received in response to the TWIC 1 NPRM, as well as recommendations from the National Maritime Security Advisory Committee (NMSAC), emphasized concerns over whether contact TWIC readers would be able to withstand the harsh conditions often present in a maritime environment. Additional concerns were raised as to whether maritime workers should be expected to remember a 6- to 8-digit PIN, especially workers who would not typically use the PIN on a regular basis. Concerns were also raised over the operational delays associated with a PIN requirement. In light of these concerns, and taking into account the level of security already provided via the TWIC's other features, the ANPRM did not propose a PIN requirement to enhance identity verification.

For card authentication, owners and operators of vessels or facilities in Risk Group A would be required to use a TWIC reader to screen individuals seeking access to secure areas. As with identity verification, owners and operators would be permitted to integrate TWIC into a PACS, provided that the owner or operator completes this integration before the TWIC-holder's information is added into the PACS, and before the TWIC-holder is granted unescorted access to secure areas.

For card validation, owners and operators of vessels or facilities in Risk Group A would be required to use a TWIC reader to check an individual's TWIC against the CCL. An owner or operator updates CCL information by downloading the current list onto the TWIC reader or PACS. At MARSEC Level 1, owners and operators would be required to update the CCL on a weekly basis. At MARSEC Levels 2 and 3, owners and operators would be required to update the CCL on a daily basis.

3. TWIC Reader Requirements for Risk Group B

The ANPRM proposed TWIC reader requirements and other TWIC-related requirements for Risk Group B that would differ depending on MARSEC Level. At MARSEC Levels 2 and 3, owners and operators of vessels or facilities in Risk Group B would be required to utilize the most protective measures of the TWIC for identity verification, card authentication, and card validation. Those requirements are the same as those described above with respect to Risk Group A.

At MARSEC Level 1, owners and operators would perform card authentication and card validation using a TWIC reader in the same manner required at higher MARSEC Levels. At MARSEC Level 1, however, owners and operators would not be required to use a TWIC reader to perform a biometric match for identity verification, subject to the exception described below. Instead, owners and operators would be permitted to perform identity verification by using the TWIC as a visual identity badge. The exception to this leniency at MARSEC Level 1 is that on a random basis, but at least 1 day per month, owners and operators would be required to perform identity verification using a TWIC reader to match the TWIC-holder's fingerprint to one stored in the TWIC.

The ANPRM's proposed requirements for Risk Group B were based on a determination that the TSI risk to such vessels and facilities at MARSEC Level 1 does not warrant a requirement to perform routine biometric identity verification using a TWIC reader.

4. TWIC Requirements for Risk Group C

The ANPRM proposed TWIC requirements for Risk Group C that would not involve the use of a TWIC reader at any MARSEC Level. Instead, owners and operators of vessels or facilities in Risk Group C would visually inspect the security features on the TWIC for identity verification, card authentication, and card validation. TWIC-holders working on vessels or at facilities in Risk Group C would periodically have their TWICs scanned using a TWIC reader during Coast Guard inspections and unannounced spot checks.

The ANPRM's proposed requirements for Risk Group C were based on our determination that, given the type of commodities and small number of passengers typical of this risk group, it is likely that these vessels and facilities present a less attractive target to individuals who wish to do harm than vessels and facilities in Risk Groups A and B. Nonetheless, vessels and facilities in Risk Group C still present some risk of being involved in a TSI. As a result, we determined that visual inspection of TWICs would be an appropriate security measure.

5. Recurring Unescorted Access

The concept of Recurring Unescorted Access (RUA) was first proposed in the TWIC 1 NPRM.[38] RUA was conceived as a means of providing flexibility to vessel owners and operators so that the TWIC program would provide them with a valuable security enhancement without unnecessarily burdening daily operations. As initially proposed, RUA would apply to vessels that would otherwise be required to use TWIC readers. RUA would allow the owners and operators of such vessels to grant certain TWIC-holders the privilege of entering secure areas on a repetitive basis without having their TWICs electronically scanned by a TWIC reader each time, provided that certain preconditions had been met.

The TWIC 1 NPRM cited two factors on which the decision to grant RUA privileges should be based: (1) The relationship of the individual to the vessel, or how well ''known'' the individual is; and (2) the individual's need to have frequent and unimpeded access to the vessel. We assumed that the crew of most vessels would consist of a relatively small number of individuals who would quickly become familiar enough with one another and readily distinguish each other from non-crewmembers. Accordingly, on such vessels, there would be no added benefit from repeated biometric identity verification using a TWIC reader.

Although RUA would exempt certain individuals from having their TWICs routinely scanned by a TWIC reader, these individuals would still need to present a TWIC for visual inspection. Additionally, prior to granting RUA privileges to a TWIC-holder, the vessel owner or operator would be required, among other things, to perform a one-time scan of the individual's TWIC using a TWIC reader for initial identity verification, card authentication, and card validity.

In addition to proposing RUA for vessels, the ANPRM also proposed RUA for facilities. Thus, owners and operators of vessels or facilities could grant RUA privileges to a number of individuals per vessel or facility.

[38] *See* 71 FR 29410–29411.

Owners and operators would be required to explain their RUA procedures in an amended security plan.

As proposed in the ANPRM and based on a recommendation from the Towing Safety Advisory Committee (TSAC), RUA could be granted to a maximum of 14 individual TWIC-holders per vessel or facility. TSAC's rationale for establishing 14 as the maximum cut off for requiring TWIC readers on vessels is that these vessels have a reduced vulnerability because the individuals are all ''known'' to one another. The number was developed by taking into account the fact that for a small vessel, such as a towing vessel or offshore supply vessel, the crew would typically include up to one Master, one Chief Engineer, and three four-person crews who rotate through watch shifts.

6. TWIC Reader Approval, Calibration, and Compliance

In the ANPRM, we considered the possibility that some owners and operators may wish to incorporate TWIC reader requirements into an existing PACS. In those situations, the ANPRM proposed to require owners and operators to follow the standard/specification to be developed from the results of the TWIC Pilot.

The ANPRM stated that we were considering alternatives for how to ensure that TWIC readers are maintained in proper working order. The existing provisions in 33 CFR 104.235, 104.260, 105.225, 105.250, 106.230, and 106.255 would require TWIC readers to be inspected, tested, calibrated, and maintained in accordance with the manufacturers' recommendations, and that records of those actions be maintained as well. The ANPRM requested comments on whether TWIC readers should be subject to additional Coast Guard inspections or third-party audits.

7. Security Plan Amendment

The ANPRM proposed a requirement on owners and operators to amend their security plans to include TWIC requirements within 6 months of promulgation of a TWIC reader final rule. In the ANPRM, we indicated that we would consider re-evaluating this deadline, and we sought public comment on how long owners and operators should have to amend security plans to incorporate TWIC reader requirements. Security plan amendments would need to detail how the owner or operator would implement TWIC requirements, including those promulgated in the TWIC 1 Final Rule, and TWIC reader requirements, if applicable.

The ANPRM mentioned that we would consider additional security plan provisions that require the owner or operator to discuss procedures for handling TWIC-holders with poor quality or no fingerprints, as well as TWIC-holders who are otherwise unable to match a live fingerprint to one of the templates stored in the card. The ANPRM also mentioned that we were considering a requirement on owners and operators using a separate PACS to explain how they will protect personal identity information.

The ANPRM articulated our position that requests for waivers, alternatives, and equivalents would need to comply with existing regulatory requirements found in 33 CFR 101.120, 101.130, 104.130, 104.135, 105.130, 105.135, 106.125, and 106.130.

In the ANPRM, we stated our intent to not amend 33 CFR 101.120 regarding Alternative Security Programs (ASPs). Instead, we would exercise our existing authority, found in 33 CFR 101.120(d)(1)(ii), to require those organizations that have approved ASPs to amend them to incorporate the TWIC requirements. Please see Section IV.C. below for a discussion on our decision to eliminate this proposal from the NPRM.

An ASP is a third-party or industry organization-developed standard that the Coast Guard has determined provides an equivalent level of security to that established by 33 CFR parts 104 or 105. MTSA-regulated facilities that are members in good standing of trade organizations or industry groups may operate under an ASP, instead of an FSP, submitted by the trade organization or industry and approved by the Coast Guard.[39] The Coast Guard permits use of ASPs to tailor Coast Guard security requirements to diverse industries within the maritime community. ASPs allow owners and operators to participate in a development process with other industry groups, associations, or organizations, and to coordinate their compliance with Coast Guard security rules and other rules already implemented.[40] Practically, ASPs are written to address a group of owners and operators based on a business model. Thus, a security standard for the small passenger industry will be different from the industry standard for container vessels, simply based on the differences in their respective vulnerabilities and associated TSI consequence. In effect, ASPs allow the end-users to implement an existing security program as an alternative to creating an individual vessel- or facility-specific security plan. ASPs also lessen the numbers of security plans that must be reviewed and approved by the Coast Guard. Currently, there are 11 approved ASPs.

8. Recordkeeping

The ANPRM proposed to require owners and operators to maintain, for a period of 2 years, records captured by TWIC readers on each scan. Under the ANPRM, owners and operators would also maintain, for a period of 2 years, records on individuals to whom RUA was granted. Finally, the ANPRM indicated that we would consider whether to require owners and operators to maintain a record to demonstrate that they have completed required card validity checks.

9. Additional Persons Required To Obtain TWICs

MTSA requires the Secretary to issue TWICs to certain individuals unless the Secretary determines that an individual poses a security risk warranting denial of the card.[41] Section 70105(b)(2) of Title 46 U.S.C. lists the categories of individuals to whom this requirement applies.

We published the ANPRM prior the enactment of the CGAA 2010. At the time we published the ANPRM, the list of individuals to whom the Secretary was required to issue a TWIC included: (1) An individual allowed unescorted access to secure areas of a MTSA-regulated vessel or facility; (2) an individual issued a license, certificate of registry, or merchant mariners document; (3) a vessel pilot; (4) an individual engaged on a towing vessel that pushes, pulls, or hauls alongside a tank vessel; (5) an individual with access to SSI; (6) other individuals engaged in port security activities; and (7) other individuals as determined appropriate by the Secretary.[42]

The Coast Guard implementing regulations in 33 CFR 101.514(a) require individuals to obtain a TWIC as a pre-condition to gaining unescorted access to secure areas of MTSA-regulated vessels and facilities. For purposes of Coast Guard regulation of these vessels and facilities, we believe that the language in 33 CFR 101.514(a) adequately covers the individuals required to obtain a TWIC. Nonetheless, at the time we published the ANPRM,

[39] *See* 33 CFR 101.125.

[40] *See* 68 FR 60449, 60454, and 60532 (October 22, 2003).

[41] 46 U.S.C. 70105(b)(1).

[42] 46 U.S.C. 70105(b)(2).

we were aware of a potential gap between MTSA and our regulations. Specifically, there may be some vessel pilots who do not hold Federal licenses, and there may be some individuals who are not credentialed mariners engaged on towing vessels that are not MTSA-regulated. Therefore, to avoid any possible gaps between MTSA and our regulations, we included a proposal in the ANPRM to explicitly include these individuals in the regulatory requirement to obtain a TWIC.

Subsequent legislation has caused us to eliminate part of this proposal from this NPRM. Section 809 of the CGAA 2010 changed the applicability of 46 U.S.C. 70105(b)(2)(B) and (D) so that the Secretary is now required to issue a TWIC to credentialed mariners and those engaged on towing vessels only if these individuals are allowed unescorted access to a secure area of a MTSA-regulated vessel. Section 809 has eliminated the gap with respect to mariners on towing vessels. Mariners who are allowed unescorted access to MTSA-regulated vessels are already covered in the existing regulatory requirement to obtain a TWIC. We no longer need to add a provision requiring mariners working on vessels that are not MTSA-regulated to obtain a TWIC. While there may be some vessel pilots that do not hold Federal licenses, we have not determined whether there is a population of State-licensed vessel pilots that are not otherwise required to obtain a TWIC because they access secure areas of MTSA-regulated vessels. We seek public comment on this subject and whether a specific provision to include them in the regulatory requirement to obtain a TWIC is necessary. If there is a population of State-licensed vessel pilots not covered under the current regulatory requirement to obtain a TWIC, we intend to revise 33 CFR 101.514 to cover that population. Please see Section IV.C. below for further discussion on our decision to eliminate or modify this proposal in this NPRM.

*E. Public Comments Received in Response to the ANPRM and Public Meeting*

This section provides a detailed discussion of the public comments received during the ANPRM's comment period and public meeting. This section also provides our responses to those comments.

We received approximately 100 comment letters in response to the ANPRM. In addition, we hosted a public meeting in Arlington, Virginia on May 6, 2009, to provide another forum for obtaining public feedback on the ANPRM.[43] Comments received at the public meeting aligned into approximately 20 categories. Copies of the public meeting sign-in sheets, written comments received, and a transcript of the public meeting, are available for viewing in the public docket for this rulemaking.

Commenters represented a wide range of individuals and entities, including: Federal, State, and local government officials; port authorities; representatives of affected industries, such as maritime, trucking, rail, security, port, and other facilities; professional/trade associations; labor unions; and private citizens. The comments received from these parties helped to inform the proposals in this NPRM.

1. General Comments

Numerous commenters supported the ANPRM's general approach to TWIC reader requirements and other TWIC-related requirements. Many recognized the potential value of the TWIC program to enhance transportation security in general, and maritime security in particular. Several commenters commended us for first publishing an ANPRM to solicit public input on a preliminary set of proposals before publishing an NPRM.

Several commenters cautioned us to implement TWIC reader requirements in a manner that does not unnecessarily burden affected industries. We believe the requirements proposed in this NPRM achieve that goal. Section V. ''Regulatory Analysis'' below provides a detailed discussion of the benefits and burdens associated with this proposed rule.

One commenter suggested that the NPRM should clarify which provisions specifically apply to vessels, and which apply to facilities. Similarly, two commenters suggested that we consider proposing separate sets of regulations for vessels and facilities.

Our proposals in this NPRM clearly distinguish between vessels and facilities. To clarify, 33 CFR part 101 sets forth general maritime security regulations, 33 CFR part 104 sets forth maritime security regulations specific to vessels, 33 CFR part 105 sets forth maritime security regulations specific to facilities, and 33 CFR part 106 sets forth maritime security regulations specific to OCS facilities. As described in greater detail below in Section IV., this NPRM proposes to add or amend relevant provisions in each of these parts. Please refer to Table ES–1 in the Executive Summary for a breakdown of the NPRM proposals by vessel, facility, and OCS facility.

Several commenters expressed general concerns about TWIC reader requirements. Some opposed any requirement to use TWIC readers, citing financial burdens and operational complications they believe would result from such requirements. Others highlighted differences between different types of vessels, and suggested that TWIC readers may not necessarily enhance security in each case. Commenters also raised concerns about increased traffic and other operational challenges associated with TWIC reader requirements.

As discussed more fully below in Sections IV. and V., this NPRM does not propose TWIC reader requirements for Risk Group B. This decision was based, in part, on comments received in response to the ANPRM. Many of the comments opposing TWIC reader requirements represented the interests of owners and operators of vessels or facilities assigned to Risk Group B. We have estimated the annualized cost of the TWIC reader requirements on vessels and facilities in Risk Group A at $26.5 million, at a 7 percent discount rate. Had we proposed TWIC reader requirements to also include Risk Group B facilities, the annualized cost would increase to $141.2 million, at a 7 percent discount rate. Moreover, including Risk Group B in the TWIC reader requirements would not only increase the annualized cost, but the average consequence figure (the monetized costs of fatalities and injuries resulting from a TSI) would drop by more than one-third. While this does not mean that there should be no TWIC reader requirements for Risk Group B, we believe this analysis supports our phased approach for requiring TWIC readers first for Risk Group A. We also wish to emphasize the utility of TWIC in enhancing security even when not used in conjunction with TWIC readers. Before mariners and other individuals were required to obtain a TWIC, they could access secure areas of MTSA-regulated vessels and facilities after presenting a State-issued driver's license or any number of other government-issued identification cards. This patchwork system of valid credentials required security personnel to become familiar with the appearance and security features of every type of acceptable credential. Moreover, since some government-issued credentials are used for purposes other than security, applicants are not necessarily screened

[43] *See* Transportation Worker Identification Credential (TWIC)—Reader Requirements, 74 FR 17444 (Apr. 15, 2009) to view the notice of public meeting; request for comments.

from a security threat perspective. Additionally, the eligibility criteria for some government-issued credentials do not preclude issuance to an individual with a felony criminal record.

The TWIC program mitigates the above shortcomings. Since April 15, 2009, TWIC has been the single credential used throughout the maritime sector. Accordingly, security personnel only need to become familiar with the appearance and security features of one credential. Moreover, unlike other government-issued credentials, TWIC is specifically designed for transportation security. Its purpose is to ensure a vetted maritime workforce by establishing security-related eligibility criteria, and by requiring each TWIC-holder to undergo TSA's security threat assessment as part of the process of applying for and obtaining a TWIC.

We will continue to analyze risk data and reassess the need to modify or add TWIC reader requirements in the future. We believe that this approach should alleviate the concerns raised by these commenters.

2. Statutory Authority

A number of commenters emphasized that the Secretary's authority to require TWIC readers on vessels is discretionary, and not mandated by MTSA. We agree with this comment.

One commenter requested clarification that if vessels in lower risk groups have not been determined by the Secretary to be at risk of a TSI, the SAFE Port Act prohibits TWIC reader requirements for such vessels. We disagree with this comment. The relevant portion of the SAFE Port Act provides: ''The Secretary may not require the placement of an electronic reader for transportation security cards on a vessel unless: (1) The vessel has more individuals on the crew that are required to have a transportation security card than the number the Secretary determines, by regulation issued under subsection (k)(3), warrants such a reader; or (2) the Secretary determines that the vessel is at risk of a severe TSI.'' [44] Under the SAFE Port Act, the Secretary could require vessels in lower risk groups to use TWIC readers if their crew size exceeds the minimum threshold, in this rule proposed as 14 individuals, established by regulation. While this NPRM does not propose TWIC reader requirements for Risk Groups B or C, the Coast Guard is not prohibited from doing so under the SAFE Port Act.

One commenter noted that certain proposals in the ANPRM would apply to facilities that receive towing vessels engaged in towing a barge or barges carrying non-hazardous cargoes, facilities that receive vessels subject to 46 CFR Chapter I, Subchapter D, that carry any flammable or combustible liquid cargoes or residue, and facilities that receive vessels not transferring cargo. The commenter suggested that these facilities are not covered by MTSA, and therefore, should not be subject to TWIC reader requirements. We disagree with the suggestion that these facilities are not covered by MTSA. MTSA broadly defines the term ''facility'' to mean ''any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States.'' [45] MTSA requires facility security plans (FSPs) for ''facilities that the Secretary believes may be involved in a transportation security incident* * *.'' [46] MTSA does not prohibit us from placing TWIC requirements on such facilities.

3. Risk-Based Approach

a. General

We received a broad range of comments with respect to the ANPRM's risk-based approach to classifying MTSA-regulated vessels and facilities. Many commenters expressed support for the ANPRM's risk-based approach. A number of commenters expressed support for a risk-based approach, but cited general reservations on the way such an approach was proposed in the ANPRM. Other commenters expressed opposition to the ANPRM's risk-based approach.

One argument cited by commenters opposing the ANPRM's risk-based approach is that vessels have already been divided into risk groups by MTSA with respect to security plan requirements, and by the Port Security Grant program. These commenters argued that to introduce another risk-based classification matrix would create too much complexity for affected industries. A larger group of commenters took the opposite view, however, arguing that the ANPRM's matrix should be based on additional variables, such as: Risk-reduction measures vessels and facilities have already implemented; size and type of vessel; port traffic volume; port location; port-wide risk; type, volume, and frequency of carrying or handling high-risk cargoes; characteristics of container cargoes and facilities; number of TWIC-holders with access to a vessel or facility; scenarios other than MSRAM's ''total destruction'' scenario; compliance costs; and other industry-specific considerations.

After considering these wide-ranging comments that fell on both sides of the issue, we continue to believe that the risk-based approach set forth in the ANPRM appropriately categorizes types of vessels and facilities based on their risk of being involved in a TSI, without creating an overly complex categorization system. Other existing risk-based categorization matrices are not tailored to TWIC requirements like the AHP/MSRAM approach described above. Additionally, as discussed more fully below in section III.G., ''HSI Report,'' HSI conducted a generally favorable independent peer review of the risk-based approach that formed the basis of the ANPRM's proposals.

Several commenters requested that the Coast Guard establish an appeals process whereby owners and operators could petition to have an assigned risk-ranking reviewed and lowered based on unique circumstances. We wish to clarify that an appeals process already exists for those directly affected by a decision or action taken pursuant to the Coast Guard's maritime security regulations.[47] Thus, owners and operators would be able to appeal a risk-ranking under the existing procedures. The establishment of a separate appeals process for petitioning TWIC-related risk-rankings is not necessary.

Other commenters suggested that COTPs should assign risk ratings to each vessel and facility on a case-by-case basis. We disagree with this approach because it is less predictable than a clear regulatory standard, and could lead to different standards being applied to similar vessels or facilities depending on their location.

b. MSRAM

Several commenters addressed the use of MSRAM as part of the ANPRM's risk-based approach. Some suggested that MSRAM should be updated to take into account risk-mitigation measures that industry has implemented since 2005. We will continue to update the MSRAM data, but we believe the data that informed the ANPRM provides an accurate basis for the regulatory proposals in this NPRM.

Other commenters requested additional information about MSRAM in order for them to comment on its utility in developing a risk-based classification system. In response, we emphasize that the ANPRM and this

[44] 46 U.S.C. 70105(m).

[45] 46 U.S.C. 70101(2).

[46] 46 U.S.C. 70103(c)(2)(A).

[47] 33 CFR 101.420; 33 CFR 104.150; 33 CFR 105.150; 33 CFR 106.145.

preamble set forth the general principles that underlie MSRAM as a risk-analysis tool. The AHP/MSRAM process generates risk scores for facility and vessel types. These scores are based on factors related to TSI consequence. Since this information is designated as SSI, the publication of more specific MSRAM data is prohibited under 49 CFR Part 15.

c. Movement Between Risk Groups

Several commenters agreed with the ANPRM's proposal to permit movement between risk groups by vessels and facilities that handle or carry dangerous cargoes only on a limited basis. Several other commenters took the opposite view, arguing that movement between risk groups would create a burdensome and confusing set of requirements, and would also introduce unfair economic incentives in favor of facilities in lower risk groups.

We continue to favor a flexible approach that allows for the option of vessels and facilities to move between risk groups based on the cargo handled or carried at a given time. This would ensure appropriate utilization of TWIC readers when dangerous cargoes are present, without imposing undue burdens when dangerous cargoes are not. Owners and operators who do not wish to take advantage of this flexibility would not be required to do so. Owners and operators who wish to take advantage of this flexibility would be expected to explain, in an amended security plan, how changes at their vessel or facility qualify for a higher or lower risk group and address the change in risk.

A number of commenters suggested alternatives to the ANPRM's approach with respect to movement between risk groups. Several argued in favor of a uniform set of TWIC requirements applicable to all vessels and facilities, which would obviate the need for regulatory provisions dealing with movement between risk groups. Two commenters suggested that facilities in Risk Group C should always retain their classification in that group, regardless of whether they handle dangerous cargoes on an infrequent basis.

We do not believe that a ''one size fits all'' approach to TWIC requirements is efficient or effective. Instead, we favor a more targeted approach that requires TWIC readers for vessels and facilities deemed higher risk, and requires less stringent TWIC requirements for vessels and facilities not deemed higher risk. We also generally disagree with an approach that would permit a vessel or facility to comply with the requirements of a lower risk group while handling or carrying cargoes that would otherwise trigger the TWIC requirements of a higher risk group. Therefore, this NPRM proposes to give the option for vessels and facilities to move between risk groups based on the cargo handled or carried at a given time.

Two commenters suggested that facilities in Risk Group C should be permitted to appeal to the COTP for a special operating designation to cover their infrequent handling of dangerous cargoes. We reiterate that an owner or operator may apply for a waiver of any requirement the owner or operator considers unnecessary, as provided in 33 CFR 104.130, 105.130, and 106.125. We also wish to note that if such a waiver is granted, an owner or operator is not required to update their security plan after approval of the waiver.

Three commenters requested clarification of the proposed TWIC requirements in scenarios where a vessel assigned to a higher risk group calls on a facility assigned to a lower risk group. One commenter suggested that, in such cases, we should allow time for TWIC infrastructures to be updated.

We wish to clarify that, according to our risk-based approach, facilities are classified by the types of commodities they handle and the types of vessels they receive. Thus, a facility that receives Risk Group A vessels would be categorized as a Risk Group A facility. We request additional comments on specific scenarios that might warrant further consideration of potential regulatory requirements to address the interaction of vessels and facilities in different risk groups.

Some commenters suggested that the regulations should provide for multiple risk group assignments within one facility for situations where one portion of the facility handles dangerous cargoes, while another portion does not. We are considering granting this request. If we grant this request, we expect the regulations to reflect that plans for multiple risk group assignments within a facility would be reviewed on a case-by-case basis and subject to COTP approval. We request additional comments from the public that specifically describe how multiple risk group assignments might apply to their facilities. We note that in the TWIC 1 Final Rule, we provided facilities with greater flexibility by revising 33 CFR 105.115 to allow owners and operators to redefine their ''secure area'' as only that portion of their access control area that is directly related to maritime transportation. We seek comments from the public on whether the additional flexibility of being able to further modify a facility's footprint by assigning different portions of the facility to different risk groups is necessary or appropriate.

d. MARSEC Levels

Several commenters agreed in principle with the ANPRM's approach of imposing enhanced TWIC requirements at higher MARSEC Levels, but questioned why there was little difference between the ANPRM's TWIC reader requirements for Risk Groups A and B at different MARSEC Levels. These commenters suggested alternative approaches, all of which were variations on the theme that TWIC reader requirements should become more stringent as MARSEC Levels are elevated. Other commenters disagreed with the ANPRM's approach, but proposed stricter requirements, suggesting that all MTSA-regulated vessels and facilities should be required to use TWIC readers at elevated MARSEC Levels. Another commenter disagreed with the ANPRM's approach, arguing that to impose different TWIC reader requirements depending on MARSEC Level is overly complex and would provide no added security benefits.

We recognize that the system of MARSEC Levels creates a useful mechanism for the Coast Guard to elevate security requirements at times of heightened risk. Nonetheless, we use this mechanism in a targeted manner, and at this time, we do not believe that elevated TWIC reader requirements at higher MARSEC Levels are generally practical or appropriate. In considering the comments above, we note the change we have made from the ANPRM to this NPRM with respect to TWIC reader requirements. In the ANPRM, we proposed TWIC reader requirements for Risk Groups A and B, with stricter TWIC reader requirements for both risk groups at higher MARSEC Levels. The ANPRM's stricter TWIC reader requirements would have primarily affected Risk Group B because the ANPRM proposed routine biometric scanning with a TWIC reader for Risk Group A at all MARSEC Levels. For example, the ANPRM would have required Risk Group B to use TWIC readers at MARSEC Level 1 for card authentication (i.e., no routine biometric scan) and once-monthly biometric identity verification. The ANPRM, however, would have only required Risk Group B to regularly use TWIC readers for biometric identity verification at higher MARSEC Levels.

In this NPRM, we have eliminated the proposed TWIC reader requirements for Risk Group B. The requirements for

routine biometric scanning with a TWIC reader for Risk Group A remain the same as in the ANPRM. Note that we propose increased requirements at higher MARSEC Levels to the extent that the NPRM would require Risk Group A to perform daily updates of CCL information at higher MARSEC Levels, instead of the weekly updates required at MARSEC Level 1.

We also note that data from the TWIC Pilot demonstrated that switching between different TWIC reader modes of operation negatively impacted the efficiency of TWIC reader use by complicating the learning process for TWIC-holders. According to the TWIC Pilot, TWIC-holders were confused by the different procedural requirements for the different TWIC reader modes of operation, regardless of attempts to inform TWIC-holders in advance of mode changes. This often resulted in delays caused by TWIC-holders' confusion as to whether or not they needed to place their finger on the TWIC reader's fingerprint sensor. In contrast, the TWIC Pilot found that when TWIC readers were used in the same mode of operation for a sustained period of time, TWIC-holders became familiar with a consistent throughput procedure, resulting in more efficient processing. While more stringent TWIC reader requirements might seem appropriate at higher MARSEC Levels, the TWIC Pilot demonstrated the importance of a consistent user experience. We also note that according to existing regulations in 33 CFR 101.405, the Coast Guard may issue MARSEC Directives setting forth mandatory measures if we determine that additional security measures are necessary to respond to specific threats.

Consistent with the findings of the TWIC Pilot, the TWIC reader requirements proposed in this NPRM call for no switching between TWIC reader modes, and also call for little variation in requirements at higher MARSEC Levels. The only difference between the requirements proposed in the ANPRM and this NPRM based on MARSEC Level is that, at MARSEC Level 1, owners and operators of vessels or facilities in Risk Group A would be required to perform card validity checks based on CCL information that has been updated weekly, whereas at higher MARSEC Levels, the CCL updates would be required daily. The increased risk associated with elevated MARSEC Levels warrants this requirement to update the CCL information more frequently. The Coast Guard seeks public comment on this approach.

e. CCL and ''Privilege Granting''

Most of the comments we received regarding the CCL recognized some benefits to card validation requirements that involve checking TWICs against this list. One commenter, however, stated that the benefits of such requirements would not outweigh the burdens. We disagree with this comment. Invalid TWICs are placed on the CCL if they are lost, stolen, damaged, or revoked by TSA for cause. The benefit of a requirement to check TWICs against the CCL is that it enables owners and operators to limit the access to secure areas of our nation's transportation system to individuals that hold a TWIC. We estimate the burden of updating CCL information into the TWIC reader or PACS to be approximately 30 minutes per week. For a more detailed discussion of the costs and benefits associated with this proposed rule, see Section V. ''Regulatory Analyses'' below.

Three commenters requested that more frequent or real-time updated CCL information be made available. These commenters argued that access to real-time CCL information would enhance security better than the method proposed in the ANPRM, which requires owners and operators to update CCL information on a weekly or daily basis depending on the particular MARSEC Level. Other commenters felt that daily or weekly download requirements are reasonable.

We believe that the requirements to download the CCL weekly or daily (based on MARSEC level) strike a reasonable balance between security and practicality. Owners and operators who wish to download CCL information more frequently would be able to do so.

Two commenters requested functionality that would enable CCL information to be downloaded directly into an entity's PACS. We confirm that this functionality exists via Internet connection.

Other commenters requested functionality that would make CCL information available through additional mechanisms, such as wireless connection to a TWIC reader, manual download to a TWIC reader, access via smart-phone, or a searchable Internet database accessible via the Homeport [48] or other secure system. We emphasize that the CCL information is available via the Internet through a wireless device or manual download to a TWIC reader.[49]

Seven commenters expressed concerns over the CCL because it groups together individuals who are legitimate security threats with individuals who merely have a lost or stolen TWIC. These commenters felt that individuals in the latter categories would be unduly stigmatized by being placed on the CCL together with individuals identified as security threats. Accordingly, they argued that the CCL should focus exclusively on individuals determined to be security threats.

We wish to clarify that the CCL does not contain names, any personally identifiable information, or any security information. The CCL is simply a list of TWIC numbers that have not yet expired, but are no longer valid for entry to secure areas due to their reported loss or theft, being revoked by TSA, or replaced administratively due to damage, or other reason.

We also note that the Coast Guard does not maintain or control the content of the CCL. The CCL is maintained and controlled by TSA. The Coast Guard has shared these comments with TSA for use in future planning. Facility and vessel owners and operators should understand that a variety of factors could cause a TWIC to be listed on the CCL.

One commenter suggested that we use a vehicle, such as the Homeport system, to notify employers when an employee has been identified as a national security threat or otherwise deemed ineligible to hold a TWIC. In response to this comment, we note that national security threats are dealt with in the manner prescribed by relevant law enforcement agencies, and typically do not involve release of any information that could compromise an ongoing investigation, including whether an individual may pose a national security threat. We also note, however, that TSA requires all TWIC applicants to acknowledge that TSA may notify employers and facility owners and operators if there is an imminent threat of risk to individuals or property.

Several commenters expressed opinions on the ANPRM's proposal regarding a ''privilege granting'' system, which would enable an owner or operator to register with TSA the names of specific TWIC-holders granted access to secure areas. TSA would then contact the owner or operator directly when a registered individual has been added to

[48] Homeport is a publicly accessible internet portal located at *https://homeport.uscg.mil,* which provides users with current maritime security information. It also serves as the Coast Guard's communication tool designed to support the sharing, collection, and dissemination of sensitive but unclassified information to targeted groups of registered users within the port population.

[49] The CCL is updated daily and is publicly available for download on the Internet at *https://twicprogram.tsa.dhs.gov/TWICWebApp/.*

the CCL. Approximately 20 commenters stated that they would prefer a privilege-granting system over a requirement to continually download or manually check CCL information. One of these commenters suggested that privilege granting should actually be a minimum requirement for all owners and operators of vessels and facilities in Risk Group C, because this would confer a meaningful security benefit at little cost. Most of the commenters supporting a privilege-granting system opposed the proposition to pay a fee for it. Two commenters suggested that if a fee were to be charged, the NPRM should include a fee estimate so that the public would have more of a basis on which to comment.

Several commenters were not in favor of the ANPRM's privilege-granting system. One simply felt it is unnecessary. Another cited employee privacy concerns. One commenter stated that a privilege-granting system might provide some benefit to vessels, but would not benefit facilities. Another stated that a privilege-granting system would not be a viable option for tug or barge operators because these operators do not know which individuals require access to which vessels or facilities.

After considering the comments and further analysis, we have decided not to include a privilege-granting system in this NPRM. The population of TWIC-holders granted access to any given vessel or facility often changes, which means that a privilege-granting system would be labor-intensive, costly, and impractical to maintain. Moreover, we believe that creating and maintaining a privilege-granting system would require substantial government and/or industry resources, and commenters were generally unwilling to pay fees that would be necessary to create and maintain such a system.

One commenter requested information on how vessels operating outside of available wireless Internet access zones would download necessary CCL updates. We wish to clarify that there would be no obligation to download updated CCL information when there are no new individuals seeking access to secure areas. For example, a vessel designated as a secure area that is underway for an extended period of time with the same crew would not need to download updated CCL information if card validity was properly confirmed when the TWIC-holders boarded the vessel. We request additional comments from the public regarding practical scenarios in which a vessel might not be able to download necessary CCL updates within the prescribed frequency (weekly or daily, depending on MARSEC Level). Additionally, we request comments from the public regarding the regulatory requirements that we should put in place when vessels are in one of those scenarios. One possibility would be to continue to require the use of TWIC readers for identity verification, card authentication, and card validity, even though the CCL might not have been updated within the prescribed frequency. This would electronically confirm that the TWIC has not expired, and also confirm no match against the most recently downloaded version of the CCL. The owner or operator would be required to update the CCL at the next available opportunity. We request comments from the public on this proposal or any preferred alternatives we should consider.

One commenter requested guidance on the obligations an employer might have if notified by TSA that a former employee's TWIC has been revoked. We wish to clarify that generally, no such notification would be forthcoming. We note, as mentioned above, that TSA requires all TWIC applicants to acknowledge that TSA may notify employers and facility owners and operators if there is an imminent threat of risk to individuals or property. In those scenarios, TSA would provide appropriate case-specific guidance to the employer at the time of any such TSA notification.

Several commenters requested additional general guidance on any proposed requirements to perform card validation using CCL information. We will consider whether and how to issue additional guidance, as necessary.

f. PIN Usage

Approximately 30 commenters agreed with the ANPRM's approach that TWIC-holders should not be required to input their PINs in order to be granted access to secure areas. Among the reasons commenters cited in opposing a PIN requirement were: intermittent use makes PINs hard to remember; difficulty of retrieving forgotten PINs; throughput delays and other disruptions; and lack of an appreciable security benefit once a biometric match has been established.

In the ANPRM, we recognized the operational and environmental challenges that a PIN requirement would present. The TWIC Pilot also noted that since many TWIC-holders had rarely, if ever, used their PINs since activating their TWICs, some workers could not remember their PINs. These individuals were then required to visit a TWIC enrollment center to reset their PINs. The TWIC Pilot also noted that inputting the PIN is not necessary to conduct a biometric match. Consistent with the comments and TWIC Pilot findings, this NPRM does not propose a requirement that TWIC-holders enter their PINs in order to access secure areas.

Several commenters also requested that PINs not be required during Coast Guard spot checks and inspections. We note that such a proposal was not included in the ANPRM. Existing regulation already requires mariners to provide their PINs to Coast Guard personnel upon request.[50] For example, when a mariner's fingerprints cannot be read using a TWIC reader, Coast Guard personnel may require the mariner to provide the PIN. To account for this and other instances when a mariner's identity cannot be verified by means other than the TWIC and PIN, we are retaining the existing provision that requires mariners to provide PIN information to Coast Guard personnel upon request.

Some commenters acknowledged that PIN verification may be useful in certain circumstances, and that there are certain advantages associated with PINs. One commenter noted that PIN usage would be a viable alternative when fingerprint matching is not possible. We agree with this comment and have addressed this issue below in section IV.F. ''TWIC Inspection Requirements in Special Circumstances.''

Another commenter suggested that TWIC readers designed to only check PINs might be less expensive than TWIC readers that perform other functions. We believe that the operational and environmental challenges presented by a PIN requirement outweigh this possible cost advantage.

One commenter stated that PINs are another line of defense against forged TWICs. We agree with this comment, but do not believe it warrants a PIN requirement. Although this NPRM does not propose to require PIN verification, owners and operators may choose to impose their own PIN verification requirement on individuals before granting them access to secure areas.

Finally, several commenters requested that we implement a more widely available and accessible system for resetting forgotten PINs. This comment relates to TSA's procedures for resetting PINs. We have provided these comments to TSA for their consideration. TSA currently protects PINs by securely locking them on the card as required by the Federal Information Processing Standards 201–1 (FIPS 201). PIN reset requires virtual private network (VPN) access to the

[50] *See* 33 CFR 101.515(d)(2).

TWIC system available only at TWIC enrollment centers. TSA is looking at possible alternatives and updates to the current PIN reset policy.

4. Utility of TWIC Readers in Reducing TSI Vulnerability

Many commenters acknowledged the utility of the TWIC program in reducing TSI vulnerability, though they expressed differing opinions on the utility of TWIC readers in that regard. Some asserted that TWIC readers would not reduce risks, especially on small vessels where crewmembers are familiar with one another, and on vessels where restricted areas are already protected by other access control mechanisms. Several of these commenters expressed the opinion that TWIC effectively reduces risk insofar as personnel are required to complete a rigorous security threat assessment in order to obtain a TWIC; yet, they believe that TWIC readers would provide no additional risk reduction benefit. Although one of these commenters acknowledged the potential utility of TWIC readers at large facilities and on large vessels, this group of commenters generally opposed all of the proposed TWIC reader requirements.

Other commenters took the opposite view. Several argued that the TWIC's security benefits would only be realized through the institution of a standard requirement to use TWIC readers at all MTSA-regulated vessels and facilities. One point emphasized by this group of commenters is that visual inspection as a means of identity verification would not effectively detect counterfeit TWICs.

One commenter favored an approach in which TWIC readers are used in addition to—not in place of—visual comparison of the TWIC-holder to the photograph on the TWIC. Another commenter favored an approach in which owners and operators would be required to conduct random electronic biometric matches using a TWIC reader, as opposed to using a TWIC reader each time an individual accesses secure areas. Finally, one commenter suggested that we include an option that would allow owners and operators to schedule periodic Coast Guard visits for the purpose of conducting comprehensive inspections using the Coast Guard's portable TWIC readers.

The wide ranging nature of these comments demonstrates the need for an analysis of the impacts of TWIC reader requirements in the maritime sector. Similarly, Congress had also mandated a thorough analysis of TWIC reader utility in the SAFE Port Act by requiring the Secretary to '' * * * conduct a pilot program to test the business processes, technology, and operational impacts required to deploy * * * [TWIC] readers at secure areas of the maritime transportation system.'' [51] At the time we published the ANPRM and received the comments above, TSA had not yet completed data collection for the TWIC Pilot. TSA completed data collection for the TWIC Pilot on May 31, 2011. In accordance with the SAFE Port Act, we crafted the proposals in this NPRM in a manner consistent with the findings of the TWIC Pilot.[52]

The TWIC Pilot was designed to assess, among other things, the utility of TWIC readers in enhancing security. The TWIC Pilot found that when designed, installed, and operated in a manner consistent with the business considerations of the vessel or facility, TWIC readers enhance security by reducing the risk that an unauthorized individual could gain access to secure areas. The TWIC Pilot also found that TWIC readers enhance security by enabling owners and operators to assign secure area access privileges to a limited population of TWIC-holders. The proposals in this NPRM to require TWIC readers are consistent with the findings of the TWIC Pilot and were developed to reduce TSI vulnerability at MTSA-regulated facilities and vessels.

5. TWIC Reader Requirements on Vessels

Many commenters expressed opposition to any requirement for TWIC readers on vessels. These commenters argued that TWIC readers on vessels would be expensive, impractical, ineffective in enhancing security, and would put U.S.-flagged vessels at a competitive disadvantage relative to foreign-flagged vessels that can operate without TWIC readers. Instead, these commenters favored using TWIC as a visual identity badge on vessels. They argued that the greatest value of the TWIC program is not as an access control device, but rather as a reliable, standardized means to establish the identity and background of new employees. The commenters emphasized that TWIC readers would likely cause logistical problems, and would be unnecessary on vessels in which crew size is relatively small, because crewmembers are familiar with one another. Finally, the commenters believed that TWIC readers are unnecessary on vessels because, in most cases, TWIC-holders accessing vessels have already had their TWICs checked using a TWIC reader at shore-side facilities and during Coast Guard inspections.

One commenter felt that there might be limited utility to TWIC readers on vessels. Another commenter proposed an alternative approach that would require vessel owners and operators to specify a certain percentage of individuals on board for random biometric matches using a TWIC reader.

As mentioned previously, we rely on the TWIC Pilot's finding that TWIC readers enhance security when used properly. Additionally, we recognize that many of the commenters arguing against the proposed requirement for TWIC readers on vessels expressed the interest of owners and operators of vessels in Risk Group B. After considering the public comments and additional analysis, we have eliminated from this NPRM the proposal to require TWIC readers on vessels in Risk Group B. As discussed more fully below in Section IV., ''Section-by-Section Description of Proposed Rule,'' this NPRM proposes TWIC reader requirements for vessels in Risk Group A only. Moreover, this NPRM proposes to exempt from TWIC reader requirements all vessels with 14 or fewer TWIC-holding crewmembers. These measures should alleviate most of the concerns raised by commenters with respect to the costs and logistics of TWIC readers on vessels and on the limits for utility on vessels with 14 or fewer crewmembers.

Some commenters expressed the opinion that on small vessels, even a requirement to use the TWIC as a visual identity badge is an unnecessary burden that would confer little or no security benefit. We disagree with this comment. A security benefit is conferred when a vessel owner or operator is able to confirm that each entrant to a secure area holds a TWIC.

One commenter requested clarification as to whether a vessel owner or operator would be required to check TWICs electronically on days the vessel does not sail. We wish to clarify that TWIC reader requirements are triggered when individuals are granted access to secure areas, regardless of whether a vessel sails.

6. TWIC Reader Requirements for Risk Group A

a. Risk Group A Classification

Two commenters questioned why Risk Group A includes facilities that handle bulk CDC, but does not include facilities that handle non-bulk Division 1.1 or 1.2 explosives. We reiterate that based on the AHP/MSRAM data and analysis, facilities that handle non-bulk

[51] 46 U.S.C. 70105(k).

[52] 46 U.S.C. 70105(k).

substances did not warrant placement in Risk Group A. Such facilities generated lower AHP scores because unlike bulk CDC, Division 1.1 or 1.2 explosives are segregated and kept in smaller quantities.

b. Risk Group A TWIC Reader Requirements

Six commenters representing owners and operators of large vessels or facilities expressed general concerns that the ANPRM's proposed TWIC reader requirements would present significant operational challenges. Another commenter stated that it would be burdensome if TWIC readers had to be manually updated to keep CCL information current.

In considering these comments, we note that the TWIC Pilot elicited a variety of lessons learned with respect to the operational impacts of deploying TWIC readers in the maritime sector. The TWIC Pilot generally found that when TWIC readers are designed, installed, and operated in a manner consistent with the business considerations of the vessel or facility, they function properly.

We believe that the proposals in this NPRM appropriately consider the findings of the TWIC Pilot and implement the TWIC reader requirements mandated by MTSA and the SAFE Port Act in a manner that enhances the nation's maritime security without imposing undue burdens. More information on the economic analysis for this proposed rule is provided below in Section V. ''Regulatory Analyses.''

We also note that in the TWIC 1 Final Rule, we revised 33 CFR 105.115 to permit owners and operators to redefine their ''secure area'' as only that portion of their access control area that is directly related to maritime transportation. This revision was intended to provide greater flexibility to facility owners and operators in dealing with the operational impacts of implementing the TWIC program at each individual facility. Additionally, as discussed above, we are also considering allowing multiple risk group designations within one facility, to account for situations where one portion of a facility handles dangerous cargoes and another portion does not.

7. TWIC Reader Requirements for Risk Group B

a. Risk Group B Classification

Numerous commenters expressed the opinion that Risk Group B is over-inclusive in terms of the types of vessels and facilities covered. Many argued that OCS facilities subject to 33 CFR part 106 do not present risks that warrant placement in Risk Group B.

Two commenters argued that tank vessels as defined in 33 CFR Subchapter D should not be placed in Risk Group B. One commenter suggested that with respect to crewmembers on Subchapter D vessels, the only requirement to scan their TWICs using a TWIC reader should be upon initial hiring at the employer's home office.

One commenter whose vessel is licensed for 800 passengers and carries a crew of six argued that TWIC reader requirements would be a financial burden that provides no appreciable security benefit. In response, we note that in this NPRM, we do not propose to require TWIC readers for Risk Group B.

One commenter argued that facilities handling no hazardous materials other than asphalt cement do not present risks that warrant placement in Risk Group B. The commenter requested that we specifically exclude from Risk Group B facilities that handle products designated as hazardous only due to storage and handling at elevated temperatures. Two commenters suggested that for purposes of this rule, the term ''hazardous materials'' should not be defined by reference to 49 CFR 172. One of these commenters argued that this definition would cover many products that present little or no risks. Instead, the commenter suggested that we adopt the definition of ''hazardous materials'' used by TSA and/or the Pipeline and Hazardous Materials Safety Administration.

We wish to clarify that the term ''hazardous materials'' is defined in 33 CFR part 101.105 as those materials subject to regulation under 46 CFR parts 148, 150, 151, 153, or 154, or 49 CFR parts 171 through 180. We believe that the types of vessels and facilities referenced in the comments above are appropriately placed in Risk Group B based on the AHP/MSRAM analysis. We further believe that the comments above seeking re-classification out of Risk Group B resulted from the ANPRM's proposal to require TWIC readers for Risk Group B. We reiterate that, based on the comments and additional analysis, this NPRM does not propose TWIC reader requirements for Risk Group B.

b. Risk Group B TWIC Reader Requirements

One commenter believed that the ANPRM's proposed requirements for Risk Group B are appropriate. Another commenter argued that identity verification upon each entry to a secure area would be too burdensome. Another commenter argued that the proposed TWIC reader requirements in the ANPRM for Risk Group B at MARSEC Level 2 would be too burdensome. Finally, two commenters argued that, as a general matter, the ANPRM's proposals are too burdensome because they would require vessels and facilities in Risk Group B to have both a TWIC reader and a security guard to visually inspect TWICs as well.

Several commenters argued that the ANPRM's requirement for Risk Group B to conduct random monthly scans using a TWIC reader would be costly and provide minimal security benefits, especially if done on a low volume or non-work day. Other commenters requested clarification as to whether the ANPRM's approach would require monthly scans on all TWIC-holders associated with a vessel or facility, or only on the TWIC-holders visiting the vessel or facility on a specific day.

Several commenters proposed alternative TWIC requirements for Risk Group B. Some suggested approaches that rely less on TWIC readers than did the ANPRM's approach. For example, two commenters suggested requiring only visual TWIC checks for identity verification, card authentication, and card validation as a routine matter at MARSEC Level 1. Thus, scans using a TWIC reader would only be required once per month at MARSEC Level 1, but would remain a standard procedure at higher MARSEC Levels. Another commenter suggested that card validity checks should be required on small vessels less frequently than as proposed in the ANPRM. Two commenters opposed the ANPRM's requirement to perform monthly scans using a TWIC reader at MARSEC Level 1.

Other commenters suggested alternative approaches that rely more on TWIC readers than did the ANPRM's approach. For example, several commenters suggested that owners and operators of vessels or facilities in Risk Group B should always be required to use TWIC readers to perform identity verification, arguing that visual checks are less reliable. Some of these commenters argued that unlike random monthly scans using a TWIC reader, routine use of TWIC readers would provide TWIC-holders the benefit of a consistent user experience.

Based on the comments and further analysis, this NPRM does not propose TWIC reader requirements for Risk Group B. We have estimated the annualized cost of the TWIC reader requirements on vessels and facilities in Risk Group A at $26.5 million, at a 7 percent discount rate. Had we proposed TWIC reader requirements to also

include Risk Group B facilities, the annualized cost would be $141.2 million, at a 7 percent discount rate. Moreover, including Risk Group B in the TWIC reader requirements would not only increase the annualized cost, the average consequence figure (the monetized costs of fatalities and injuries resulting from a TSI) drops by more than one-third. While this does not mean that there should be no TWIC reader requirements for Risk Group B, we believe this analysis supports our phased approach for requiring TWIC readers first for Risk Group A.

We also wish to emphasize the utility of TWIC in enhancing security even when not used in conjunction with TWIC readers. Before mariners and other individuals were required to obtain a TWIC, they could access secure areas of MTSA-regulated vessels and facilities after presenting a State-issued driver's license or any number of other government-issued identification cards. This patchwork system of valid credentials required security personnel to become familiar with the appearance and security features of every type of acceptable credential. Moreover, since some government-issued credentials are used for purposes other than security, applicants are not necessarily screened from a security threat perspective. Additionally, the eligibility criteria for some government-issued credentials do not preclude issuance to an individual with a felony criminal record.

The TWIC program mitigates the above shortcomings. Since April 15, 2009, TWIC has been the single credential used throughout the maritime sector. Accordingly, security personnel only need to become familiar with the appearance and security features of one credential. Moreover, unlike other government-issued credentials, TWIC is specifically designed for transportation security. Its purpose is to ensure a vetted maritime workforce by establishing security-related eligibility criteria, and by requiring each TWIC-holder to undergo TSA's security threat assessment as part of the process of applying for and obtaining a TWIC.

As we go forward with our phased approach to implementing TWIC reader requirements, we will continue to evaluate the use of TWIC readers on vessels and at facilities, and determine the need for additional or different TWIC reader requirements. Proposing requirements for Risk Group A only in this NPRM is indicative of our desire to minimize highest risks first, but should not be read to foreclose revised TWIC reader requirements in the future.

Several commenters argued that container (cargo) facilities present risks that actually warrant the more stringent TWIC reader requirements of Risk Group A rather than those of Risk Group B. In response, we note that, based on the AHP/MSRAM analysis, being a container facility alone did not automatically cause a facility to be categorized in Risk Group B. In addition, several factors led the Coast Guard to decide not to require TWIC readers for most of these facilities at this time. First, there are limits on the additional risk reduction (above and beyond the credentialing and visual identification purposes of the TWIC itself) of TWIC readers at container facilities. Security risk in the maritime sector can be considered as following one of three high-level scenarios: (1) The asset in question could be the target of an attack; (2) the asset in question could be used as a weapon for an attack; or (3) the asset could be used to enable or facilitate an attack elsewhere. For container facilities, the first scenario brings low risk given the number of personnel concentrated and exposed to an attack and limited storage of hazardous materials. Similarly, the second scenario brings low risk as containers bring low risk of use as a weapon. Furthermore, the use of TWIC readers, or other access control features, would not mitigate the threat associated with the contents of a container. The TWIC reader serves as an additional access control measure, but would not improve screening of cargoes for dangerous substances or devices. The third scenario is the primary risk driver for container facilities, with the risk of containers used to smuggle illicit materials and/or personnel into the country. The additional verifications provided by TWIC readers, however, would bring limited utility to this scenario. Those individuals looking to access the contents of the container could do so after the container exits the secured area. As such, TWIC readers bring limited additional risk reduction over the TWIC itself. Additionally, requiring TWIC readers at container facilities brings significant costs, as these facilities typically have a higher number of access points per facility (and therefore would incur more capital costs) and higher numbers of personnel accessing the facility. While the additional time to use the TWIC reader to conduct a biometric match over the visual inspection is limited on an individual basis, the high volume of workers could cause the associated delay costs to accrue to much more significant levels than other facility types. Given the large numbers of truck drivers accessing these facilities, these delays would also be accompanied by increased air emissions, resulting in greater potential for environmental impact. Therefore, in this NPRM, only those container facilities that are otherwise categorized in Risk Group A would be required to use TWIC readers. We will continue to assess whether container facilities warrant additional consideration with respect to TWIC reader requirements. We welcome additional comments from the public on the risk group classification of container facilities.

8. TWIC Requirements for Risk Group C

a. Risk Group C Classification

One commenter supported the ANPRM's classification of OSVs in Risk Group C. One commenter suggested that the passenger cutoff number for vessels in Risk Group C should not be 500. Instead, this commenter argued that the cutoff number should be 49 overnight passengers or 150 passengers, similar to the Coast Guard's vessel safety regulations. In response, we reiterate that the AHP/MSRAM analysis considered factors based on TSI consequence. These factors are different than the factors that underpin the Coast Guard's safety regulations. The passenger cutoff numbers derived from the AHP/MSRAM analysis are more appropriate for defining the risk-based framework for TWIC reader requirements.

b. Risk Group C TWIC Requirements

Many commenters agreed with the ANPRM's approach that TWIC reader requirements would not appreciably enhance security for vessels and facilities in Risk Group C. One commenter further argued that since vessels and facilities in Risk Group C are so low risk, even visual TWIC inspections would be an unnecessary burden that would confer no security benefit. As noted above, however, several commenters took the opposing view, broadly asserting that owners and operators of all MTSA-regulated vessels and facilities (including those in Risk Group C) should be required to use TWIC readers to control access to secure areas.

We believe that although vessels and facilities in Risk Group C present a less likely target for individuals wishing to do harm, these vessels and facilities still hold the potential of being involved in a TSI and with consequences that could still be significant. A security benefit is conferred when an owner or operator is able to confirm that each entrant to secure areas holds a TWIC, as the TWIC serves as evidence that the person has

successfully passed TSA's security threat assessment. Accordingly, this NPRM proposes the same requirements as the ANPRM for Risk Group C, which includes requirements to visually inspect TWICs before granting unescorted access to secure areas, as is already required in the current regulations.

Some commenters asked whether vessels and facilities in Risk Group C would need dedicated security guards to perform visual TWIC checks, and what credentials these security guards would need to possess. Under current regulations (which would not change under this NPRM) for vessels and facilities categorized in this NPRM as Risk Group C, security personnel must visually inspect the TWIC of each person seeking unescorted access to secure areas. Our regulations do not require the use of ''dedicated security guards,'' but do require that the security personnel doing visual inspection of TWICs have certain knowledge, training, and experience. It is important for owners, operators, and others with security duties to be familiar with the technologies embedded in the TWIC, particularly the features that make the TWIC resistant to tampering and forgery. Those who would be examining TWICs at access control points should be familiar enough with the TWIC's physical appearance so that variations or alterations are easily recognized. Relevant security training requirements for personnel on vessels and at facilities are found at 33 CFR 104.210, 104.215, 104.220, 104.225, 105.205, 105.210, 105.215, 106.205, 106.210, 106.215, and 106.220.

9. Physical Placement of TWIC Readers

Eight commenters requested clarification as to whether TWIC readers would be required at the access points to each secure area or at the perimeter access points to the vessel or facility. Three commenters suggested that vessels should not be required to place TWIC readers at every access point to a secure area. Instead, according to these commenters, vessels required to have TWIC readers should only be required to place them at the main access points to the vessels. Several commenters expressed concerns that if TWIC readers are required at the access points to each secure area on vessels, safety would be compromised in emergency situations when crewmembers need immediate access to those areas.

We wish to clarify that for both vessels and facilities, the term ''secure area'' is defined as ''* * * the area * * * over which the owner/operator has implemented security measures for access control * * *. It does not include passenger access areas, employee access areas, or public access areas * * *.'' [53] For facilities, the secure area may encompass the entire facility, or the facility may consist of a combination of secure areas and public access areas. Similarly, for vessels, the secure area may encompass the entire vessel, or the vessel may consist of a combination of secure areas and passenger and employee access areas.

This NPRM proposes different requirements for vessels and facilities with respect to the placement of TWIC readers. For facilities, this NPRM proposes to require TWIC readers at the access points to each secure area. If the entire facility is designated as a secure area, then TWIC readers would only be required at the access points to the facility itself. If the secure area does not encompass the entire facility, then TWIC readers would be required at the access points to each secure area.

For vessels, this NPRM proposes to require TWIC readers at the access points to the vessel itself, regardless of whether the secure area encompasses the entire vessel. Thus, even if the secure area does not encompass the entire vessel (e.g., a passenger vessel consisting of secure areas and passenger and employee access areas), TWIC readers would only be required at the access points to the vessel itself. TWIC-holders may be granted unescorted access to the vessel's secure areas after the TWIC has been verified, validated, and authenticated at a vessel access control point. TWIC-holders may then move between secure areas and passenger and employee access areas without processing through a TWIC reader each time. We request additional comments from the public on the proposed regulatory provisions regarding the placement of TWIC readers for vessels and facilities, and how to minimize crewmembers from entering secure and/or restricted areas if they do not hold a TWIC.

With respect to emergency situations, we partially addressed this issue in the TWIC 1 Final Rule, and added a paragraph to 33 CFR 101.514 clarifying that emergency personnel need not have TWICs to obtain unescorted access to secure areas during emergencies. Moreover, this NPRM does not propose to require TWIC readers on vessels at each access point to a secure area. Instead, TWIC readers would only be required at the access points to the vessel itself.

One commenter suggested that with respect to OCS facilities, the appropriate location for TWIC reader placement is not on the facility itself, but, rather, at the shore-side points of embarkation for the facility. This comment echoes a recommendation from NMSAC in the TWIC 1 NPRM,[54] to which we responded that OCS facilities where access is limited and can be controlled by reading the TWIC at the point of embarkation may continue to do so. Note that this NPRM does not propose TWIC reader requirements for any OCS facilities. Accordingly, OCS facilities where access is limited and can be controlled by visually inspecting the TWIC at the point of embarkation may do so.

One commenter suggested that owners and operators of facilities should not be required to use TWIC readers on docks and other waterside access points. In response, we emphasize that we are not proposing a blanket exemption from TWIC reader requirements on docks and other waterside access points. As proposed in this NPRM, owners and operators of facilities in Risk Group A would be required to ensure that access to secure areas is limited to individuals whose TWICs have been scanned by a TWIC reader.

We also note that in the TWIC 1 Final Rule, we revised 33 CFR 105.115 to provide greater flexibility to facility owners and operators by allowing them the option to redefine their ''secure area'' as only that portion of their access control area that is directly related to maritime transportation. Thus, facilities whose footprint includes portions that are not directly related to maritime transportation can submit an FSP for Coast Guard approval that removes those areas from the definition of the facility's ''secure area'' for Coast Guard regulatory purposes. Such facilities would typically include refineries, chemical plants, factories, mills, power plants, smelting operations, or recreational boat marinas. As discussed above, we are also considering allowing multiple risk group designations within one facility, to account for situations where one portion of a facility handles dangerous cargoes and another portion does not. Owners and operators should comply with TWIC reader requirements in a manner that considers the specific nature of their facilities and their access points, and they may take advantage of regulatory provisions that would minimize the impact on operations.

10. Recurring Unescorted Access

Numerous commenters generally supported the ANPRM's provision

[53] 33 CFR 101.105.

[54] *See* 71 FR 29405.

regarding RUA as a means of providing relief to owners and operators otherwise required to use TWIC readers. Many of these commenters expressed differing opinions regarding the proposed cutoff number of 14. Six commenters stated that 14 is an appropriate cutoff number. More than 25 commenters felt that the cutoff number should be higher. One commenter felt that the cutoff number should be lower. Several commenters argued that 14 is an arbitrary cutoff number, though they offered no rationale or alternative cutoff number. Five commenters suggested that the cutoff number should be approved by the COTP on a case-by-case basis, considering factors such as an entity's size and whether a vessel operates with multiple crews.

Several commenters requested clarification regarding whether an entity could grant RUA privileges to contractors, vendors, and other frequent visitors.

Approximately eight commenters opposed the ANPRM's RUA proposal, suggesting instead that we should simply exempt all vessels with fewer than 14 TWIC-holders on board from TWIC reader requirements. One commenter noted that such an exemption would fall squarely within the SAFE Port Act's provision that prohibits requiring TWIC readers on vessels that the Secretary has determined do not have the requisite number of TWIC-holders as crewmembers.[55]

Two commenters argued that RUA would compromise security by granting unescorted access to secure areas without requiring individuals to undergo screening using a TWIC reader.

One commenter felt the phrase ''recurring unescorted access'' could be misinterpreted to mean that an individual may require an escort to access a secure area, even if the individual is a TWIC-holder.

Several commenters opposed a requirement to perform the initial biometric scan using a TWIC reader on TWIC-holders granted RUA. Their rationale was that TSA already performs reliable biometric identity verification prior to the issuance of each individual's TWIC. Some commenters also raised concerns of potential fraud that could arise if, as suggested in the ANPRM, an owner or operator pursued an agreement with a facility or other company to borrow or otherwise have access to a TWIC reader in order to perform the one-time initial biometric verification.

One commenter felt that the proposed initial biometric scan requirement would be appropriate. Another commenter felt that owners and operators should be required to perform an electronic biometric scan using a TWIC reader at the beginning of each shift for each TWIC-holder granted RUA.

Three commenters argued that owners and operators granting RUA privileges should not be required to purchase a TWIC reader to perform initial biometric scans on RUA grantees. Two commenters suggested that an Internet-based system would provide the most practical method for keeping track of RUA grantees.

One commenter called attention to the fact that employee records regarding individuals granted RUA would be kept by the employer, not the Coast Guard or TSA.

After considering the comments and further analysis discussed below in Section IV., ''Section-by-Section Description of Proposed Rule,'' we have removed from this NPRM the RUA provisions proposed in the ANPRM. RUA was previously proposed to introduce flexibility and provide relief to vessels otherwise required to use TWIC readers, based on the familiarity that exists between a relatively small number of crewmembers. This NPRM incorporates two important proposals, however, that render RUA an unnecessary provision. First, unlike the ANPRM, which proposed TWIC reader requirements for Risk Groups A and B, this NPRM proposes TWIC reader requirements for Risk Group A only. Second, this NPRM proposes a broad exemption from TWIC reader requirements for all vessels with 14 or fewer TWIC-holding crewmembers. This exemption is based on the SAFE Port Act's provision that prohibits requiring TWIC readers on vessels that the Secretary has determined do not have the requisite number of TWIC-holders as crewmembers.[56] These two changes render the need for RUA as a mechanism for regulatory relief unnecessary.

11. TWIC Reader Durability, Safety, Approval, Calibration, and Compliance

Four commenters expressed concerns that harsh weather and other physical stresses on vessels and at facilities would likely cause TWIC readers to fail or otherwise become damaged. One commenter countered that TWIC readers have already been subjected to environmental testing, and have proven to function well in the marine environment.

The TWIC Pilot found that at varying locations, some TWIC readers experienced difficulty scanning fingerprints in inclement weather. Certain types of TWIC readers withstood harsh weather conditions, whereas others were found to be sensitive to those conditions. Throughout the TWIC Pilot, the conditions under which TWIC readers had to perform were significantly more challenging than those commonly found at entrances to office buildings and other more controlled locations and environments. The TWIC Pilot, however, noted that most of the challenges associated with weather can be overcome with proper planning that takes environmental conditions into consideration.[57]

One commenter requested that we consider the safety concerns of using TWIC readers in areas where flammable materials are stored or transferred. We agree that safety concerns are of the utmost importance, and expect that owners and operators who carry or handle flammable materials would comply with applicable TWIC reader requirements in a manner that does not compromise safety.

One commenter stated that TWIC readers must be able to process biometric scans in 3 seconds or less in order to minimize the impact of TWIC reader requirements at facilities with large numbers of entrants. Several commenters stated that we should establish a minimum standard for errors in connection with TWIC reader technology. We have passed these comments to TSA for consideration in future planning. TSA has established the TWIC reader specifications and Qualified Technology List process (described later in this section) to validate that TWIC readers meet the specifications. In addition, TSA is conducting a card error/failure analysis to identify and address TWIC reader and card failures. There is additional information on TWIC reader throughput in the TWIC Pilot report, which is available in the public docket for this rulemaking.

As discussed in the ANPRM, TWIC readers are considered ''security systems and equipment,'' and therefore, existing regulatory provisions applicable to security systems and equipment maintenance would require that TWIC readers be inspected, tested, calibrated, and maintained in accordance with the manufacturers'

[55] 46 U.S.C. 70105(m)(1).

[56] 46 U.S.C. 70105(m)(1).

[57] See page vii of the TWIC Pilot Report. (A copy of the TWIC Pilot Report is available for viewing in the public docket for this rulemaking.)

recommendations.[58] Additionally, records of such actions would be required to be maintained for at least 2 years and made available to the Coast Guard upon request.[59] The ANPRM sought public comment on whether TWIC readers should also be subject to additional Coast Guard inspections and/or third party audits to further ensure that TWIC readers are maintained in proper working order.

Two commenters favored both additional Coast Guard inspections and third-party audits to check that TWIC readers are maintained in proper working order. Ten commenters opposed third-party audits, and suggested that the Coast Guard should conduct compliance inspections. Six commenters favored neither Coast Guard inspections nor third-party audits, arguing that owners and operators are already required to maintain security equipment maintenance logs, which can be reviewed by the Coast Guard to make compliance determinations. We note that 33 CFR 104.260 and 105.250 already require security systems (which would include TWIC readers) to be in good working order and inspected, tested, calibrated, and maintained according to the manufacturer's recommendation. These existing regulatory provisions also require owners and operators to maintain records of the results of such testing for 2 years. Additionally, Coast Guard field inspectors would inspect TWIC reader functionality as part of regularly occurring inspections. We agree with the majority of commenters above that appreciable value would not be added by requiring additional Coast Guard inspections and/or third party audits beyond the existing provisions on security systems and equipment maintenance. Therefore, this NPRM does not propose additional Coast Guard inspections and/or third party audits.

One commenter generally requested guidance regarding how owners and operators may voluntarily use TWIC readers before we publish a TWIC reader final rule. On March 15, 2011, we published a notice announcing the availability of Policy Advisory Council Decision (PAC–D) 01–11, ''Voluntary Use of TWIC Readers,'' [60] providing guidance on how owners and operators may use TWIC readers to meet existing regulatory requirements. Navigation and Vessel Inspection Circular (NVIC) 03–07 [61] provides additional guidance to the public on this issue.

Five commenters requested that we immediately publish a list of TWIC reader specifications, or a list of acceptable TWIC reader vendors, so that owners and operators wishing to use Federal grant money to purchase equipment can do so before we publish a TWIC reader final rule. Another commenter cautioned that such an approach may not be advisable because TWIC reader technology is still evolving.

PAC–D 01–11 provides guidance on how owners and operators of vessels or facilities can use TWIC readers to meet existing regulatory requirements for effective identity verification, card validity, and card authentication. A list of TWIC readers that have passed the Initial Capability Evaluation (ICE) Test is available at *http://www.tsa.gov/assets/pdf/twic_ice_list.pdf.* As stated in PAC–D 01–11, however, TWIC readers allowed pursuant to PAC–D 01–11 may no longer be valid after promulgation of a TWIC reader final rule, and DHS will not fund replacement TWIC readers.

The Department of Commerce's National Institute of Standards and Technology (NIST) and TSA are developing TWIC reader specifications. TSA will establish a process to qualify TWIC readers, and will maintain a Qualified Technology List (QTL) of acceptable TWIC readers. We anticipate that there may be changes from the ICE Test list to the QTL list, based on final TWIC reader specifications resulting from the QTL process.

12. TWIC Pilot and HSI Report

Seven commenters expressed confidence that the TWIC Pilot would yield important information that should inform this NPRM, including information regarding TWIC reader error rates, transaction times, durability in extreme weather conditions, and TWIC integration with an existing PACS. Two commenters requested that the TWIC Pilot include additional ports. The Merchant Marine Personnel Advisory Committee (MERPAC) recommended that the TWIC Pilot should include a sufficient number of vessels in appropriately diverse operating areas to test TWIC reader technology, operating conditions, and procedures.

TSA completed data collection for the TWIC Pilot on May 31, 2011. The TWIC Pilot gathered data from pilot sites regarding TWIC reader performance and reliability as well as throughput data at vehicle and pedestrian access points, which was instrumental in evaluating the impact of TWIC reader use on vessel and facility operations. Although the SAFE Port Act required the pilot program to take place at not fewer than five distinct geographic locations, the program actually took place in seven geographic locations to allow for the evaluation of TWIC reader functionality and impacts across a variety of environmental and operational conditions. The TWIC Pilot report provides a list of the TWIC Pilot participants.

Two commenters urged us to consider the final HSI Report in crafting the NPRM. We acknowledge that the HSI Report has provided useful insights and information that have informed the proposals in this NPRM.

A summary of both the TWIC Pilot and HSI Report recommendations are provided below in Sections III.F. ''TWIC Reader Pilot Program'' and III.G., ''HSI Report,'' respectively. A copy of the TWIC Pilot Report is available for viewing in the public docket for this rulemaking. A non-SSI version of the HSI Report is available for viewing in the public docket for this rulemaking.

13. Security Plan Amendment

Two commenters requested that the revisions to security plans resulting from this NPRM should be as minimal as possible. We believe the proposals in this NPRM are consistent with that request.

Six commenters generally supported the ANPRM's proposal to require amendments to security plans within 6 months after we publish a final TWIC reader rule. Three commenters felt that the ANPRM's proposed deadline of 6 months is too short. One commenter requested a 9-month deadline. Five commenters requested at least a 1-year deadline. One commenter suggested staggered deadlines of 24 months, 18 months, and 12 months for Risk Groups A, B, and C, respectively. Six commenters requested staggered deadlines based on the expiration dates of existing security plans. Two commenters suggested that each security plan amendment deadline should be determined on a case-by-case basis. Another commenter suggested that requirements to amend security plans should apply once we have classified each vessel and facility into its risk group.

In light of the comments and further analysis, this NPRM would extend the proposed deadline for security plan updates. Owners and operators would

[58] *See* 33 CFR 104.260 and 105.250.

[59] *See* 33 CFR 104.235 and 105.225.

[60] Policy Advisory Council Decision 01–11, ''Voluntary Use of TWIC Readers,'' available for viewing at *https://homeport.uscg.mil/.*

[61] *See* Navigation and Vessel Inspection Circular (NVIC) No. 03–07, ''Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector,'' (July 2, 2007).

be required to amend security plans to include TWIC requirements within 2 years after publication of the final rule in the **Federal Register**.

One commenter suggested that amended security plans should be reviewed by the Coast Guard before owners and operators are required to invest resources into TWIC-related expenditures. We encourage owners and operators to work with the Coast Guard, as needed, to prepare security plans that comply with regulatory requirements. We do not believe, however, that it is necessary to create a formal coordination process in which the Coast Guard would review amended security plans separate from what already exists.

14. Recordkeeping

The ANPRM proposed a requirement on owners and operators using TWIC readers to maintain records on each individual granted unescorted access to a secure area. Owners and operators would be required to maintain such records for a period of 2 years. Five commenters argued that owners and operators should not be required to check the TWICs of individuals leaving a vessel or facility. This is consistent with the ANPRM's approach, and we propose it in this NPRM as well.

One commenter considered the ANPRM's proposed 2-year record retention requirement to be reasonable. Other commenters believed 2 years is longer than necessary for record retention, and suggested alternative durations ranging from 30 days to 1 year. Fifteen commenters opposed a 2-year record retention requirement altogether, arguing that the costs would outweigh the benefits to law enforcement. One commenter opposed recordkeeping requirements for Risk Group C.

We believe TWIC reader records can prove useful to law enforcement without imposing an undue burden on the regulated population. The 2-year timeframe for record retention was designed, in part, for consistency with existing security-related and other recordkeeping requirements applicable to vessels and facilities.[62] A uniform timeframe for recordkeeping requirements provides the public with a consistent and predictable standard.

Two commenters stated that MTSA does not require the Secretary to impose recordkeeping requirements. We agree with this comment. With respect to TWIC, MTSA requires the Secretary to prescribe regulations to prevent an individual from entering secure areas of vessels and facilities unless the individual is so authorized and either possesses a TWIC or is escorted by someone who possesses a TWIC.[63] Thus, while MTSA does not specifically require the Secretary to impose recordkeeping requirements, such requirements are within the Secretary's authority, and they are an important part of the set of regulations designed to prevent unauthorized access to the secure areas of the nation's transportation system. For example, in the event of a TSI or a security breach, records would be available to the Coast Guard and other law enforcement to enable them to determine who had accessed the vessel or facility.

Two commenters requested that we prescribe more detailed recordkeeping requirements. In contrast, one commenter requested that we allow individual regulated parties to determine the best method and manner of complying with the recordkeeping requirements. We agree with the latter commenter's more flexible approach.

One commenter acknowledged that TWIC-related records could be useful to law enforcement, but argued that records should only be shared with law enforcement on a need-to-know basis. Another commenter suggested that records should only be kept to the extent they provide a homeland security-related benefit. We believe that TWIC reader recordkeeping requirements would prove beneficial to law enforcement in any number of investigations. Accordingly, this NPRM does not propose restrictions on how law enforcement may use those records.

One commenter questioned whether portable TWIC readers have the capability to retain records for 2 years. In response to this question, we wish to clarify that this NPRM would not require records to be stored specifically in TWIC readers. Logs from TWIC readers may be maintained on the TWIC readers themselves or exported to other systems. As stated above, we are not prescribing the specific method and manner of complying with the proposed recordkeeping requirements.

Four commenters expressed concerns regarding the privacy of personal information stored in TWIC readers. Some commenters highlighted concerns with respect to foreign-owned vessels and vessels traveling in foreign waters where equipment may be subject to seizure by foreign authorities. One commenter suggested that the personal information stored in a TWIC reader should be classified as SSI, which would trigger the compliance protections in 49 CFR part 1520.

We believe that information collected by a TWIC reader needs to be protected. We wish to clarify that the TWIC requirements found in 33 CFR part 104 do not apply to foreign vessels.[64] We also wish to clarify that TWIC readers typically do not capture or record the name of the TWIC-holder. A TWIC reader only captures the TWIC-holder's name if it is a contact TWIC-reader (i.e., one that requires the TWIC-holder to insert the TWIC into a slot for direct contact between the TWIC reader and the chip embedded in the TWIC) and only after the TWIC-holder has entered the PIN. This NPRM does not propose to require owners and operators to specifically use contact TWIC readers, nor does this NPRM propose any PIN requirement. Therefore, a TWIC reader will typically capture three pieces of information when an individual's TWIC is scanned: (1) FASC—N; (2) date; and (3) time. As explained above, a contact TWIC reader will also capture name information after the PIN has been entered. A PACS may also capture the name of the TWIC-holder. We consider a TWIC-holder's name and FASC–N to be SSI under 49 CFR 15.5. Therefore, if that information is captured by a TWIC reader, the information would need to be protected in accordance with 49 CFR Part 15, which imposes duties on ''certain covered'' persons to protect SSI.[65] ''Covered persons'' include, among others: (1) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law; (2) each owner or operator of a maritime facility required to have a security plan under MTSA and each person who has access to SSI, as specified in 49 CFR 15.11.[66] Furthermore, the International Ship and Port Facility Security Code requires a vessel's security plan and applicable security records to be protected from unauthorized access or disclosure.[67] SSI information collected by a TWIC reader falls under that requirement.

One commenter supported the ANPRM's proposed requirement that owners and operators explain how they are protecting personal identity information stored in a separate PACS. Two commenters questioned whether MTSA grants the Coast Guard authority to impose such a requirement.

To the extent that a PACS contains personal identity and biometric

[62] 33 CFR 104.235; 33 CFR 105.225.

[63] 46 U.S.C. 70105(a).

[64] *See* 33 CFR 104.105(d).

[65] *See* 49 CFR 15.7.

[66] *See* 49 CFR 15.7.

[67] *See* International Ship and Port Facility Code, Part A, adopted on December 12, 2002, Sections 9.7, 9.8 and 10.4.

information, it contains SSI, which must be protected in accordance with 49 CFR part 15. The Coast Guard, through delegation from the Secretary, has the authority to impose such recordkeeping requirements. Section 70124 of Title 46 U.S.C. authorizes the Secretary to issue regulations necessary to implement provisions of chapter 701 of Title 46 U.S.C, and 46 U.S.C. 70103(c)(4) subjects all security plans to review by the Secretary. Additionally, 46 U.S.C. 71013(c)(4)(D) requires the periodic verification of the effectiveness of an FSP. Recordkeeping requirements are authorized under those statutory provisions.

15. Other Comments

Seven commenters requested additional public meetings and greater coordination between the Coast Guard and affected industries as the TWIC program is implemented. Two commenters requested greater labor union input regarding the employee information collected and stored in the TWIC. One commenter requested greater Coast Guard collaboration with Congress, authorities from affected States, and Coast Guard advisory committees during the rulemaking process.

We will hold at least one public meeting in connection with this rulemaking and we are considering holding additional public meetings in connection with this rulemaking. The details of any future public meeting will be published in a separate notice in the **Federal Register**. We welcome the participation and comments of all interested parties.

Three commenters suggested that TWIC reader requirements should be tailored to enable integration with an existing PACS, since some owners and operators have invested substantial resources into existing systems. We agree with these commenters. In fact, data from the TWIC Pilot demonstrated that those pilot participants where TWIC readers were certified for operation with an existing PACS encountered fewer integration and operational and technical issues than other pilot participant systems. Accordingly, this NPRM proposes options for vessels and facilities to either use a stand-alone TWIC reader or to integrate TWIC into an existing PACS.

Two commenters requested additional information regarding the ANPRM's reference to alternate biometrics that may be used in connection with TWIC. This NPRM continues to propose two alternatives for biometric matching. Owners and operators may: (1) Use a TWIC reader to match the TWIC-holder's fingerprint to one of the fingerprint templates stored in the TWIC; or (2) use a PACS to match the TWIC-holder's biometric to the biometric stored in a PACS. For the latter option, owners and operators may use a different biometric than the fingerprint, such as an iris scan or hand geometry, stored in a PACS to be matched to the individual seeking access to secure areas. Since the implementation of the latter option would be unique to each vessel or facility, it would be impractical for us to propose a single set of prescriptive regulations for each owner and operator to follow. Instead, owners and operators would explain in their security plans the details of how their use of alternate biometrics performs the required access control functions.

Two commenters suggested that TWIC functionality should be enhanced to include other biometrics in addition to fingerprints. We believe that to enhance the features on the TWIC so that it includes other biometrics in addition to fingerprints would increase the costs associated with the TWIC program. We do not currently have data to show that the benefits of such an enhancement would justify those additional costs. Furthermore, the only standard for a biometric that the Federal government has published to date is the fingerprint biometric.[68]

One commenter suggested that the final TWIC reader rule should become effective only after a period of 24–36 months to enable owners and operators to adequately train employees and test their TWIC readers. We acknowledge that a period for TWIC reader training and testing is warranted. This NPRM proposes an effective date for compliance within 2 years after publication of a TWIC reader final rule in the **Federal Register**.

One commenter requested confirmation that the regulations are imposing minimum requirements, and that owners and operators be given discretion to implement higher standards. While we have sought to minimize costs in this rulemaking, owners and operators may impose security provisions that exceed the minimum regulatory requirements.

Three commenters suggested that vessels operating outside U.S. waters should not be required to use TWIC readers, citing concerns about disruptions at foreign ports due to the inability of foreign workers to access these vessels. We disagree with these comments and do not propose an exemption from TWIC reader requirements for vessels operating outside U.S. waters. Under existing regulation, all persons requiring unescorted access to secure areas of a MTSA-regulated vessel must possess a TWIC, regardless of whether the vessel is located in U.S. waters.[69] For any individual without a TWIC to access secure areas of a MTSA-regulated vessel, the individual must be authorized to be there and also be escorted by a TWIC-holder.

One commenter asked whether a non-U.S. citizen is eligible to obtain a TWIC. A list of certain non-U.S. citizens that are eligible to obtain a TWIC is available on TSA's Web site at *http://www.tsa.gov/sites/default/files/publications/pdf/twic/immigration_status_documents.pdf.*

Some commenters requested additional guidance for situations when TWIC readers or communication systems malfunction. In this NPRM, we propose that, in the event of a TWIC reader malfunction, individuals can still be granted unescorted access to secure areas for a period not to exceed 7 days, provided that the individual has been granted such unescorted access in the past and is known to possess a TWIC. Owners and operators expecting such occurrences should provide appropriate contingency planning in their security plans. We request comments from the public regarding whether 7 days is a sufficient amount of time in which to expect resolution of a typical TWIC reader or communication systems malfunction.

Four commenters requested further guidance with respect to how owners and operators would be required to process TWIC-holders with poor quality or no fingerprints. In such instances, we expect that the owner or operator would describe in their security plan the exception process they plan to use. The exception process may include PIN verification, alternative biometric verification, visual comparison of the digital photo stored in the TWIC to the presenter using a portable reader with a contact interface and releasing the photo to the reader screen by entering the 6-, 7-, or 8-digit PIN, or an alternative process proposed by the owner or operator and approved by the Coast Guard.

Three commenters argued that TWIC reader requirements at rail entrances to facilities would be impractical. These

[68] *See* National Institute of Standards and Technology (NIST) Special Publication 800–76–1, ''Biometric Data Specification for Personal Identity Verification,'' (January 2007), available at *http://csrc.nist.gov/publications/nistpubs/800–76–1/SP800–76–1_012407.pdf.*

[69] *See* 33 CFR 101.514.

commenters cited throughput delays, increased traffic, environmental concerns with increased emissions, costs of TWIC readers at seldom-used rail entrances, and security risks when rail workers leave their cargoes unattended to walk to the nearest TWIC reader.

We note that facilities could provide TWIC-holding escorts to rail workers, which is one way to alleviate these concerns. We also note that current regulations already require visual inspection of TWICs at rail entrances to secure areas of regulated facilities. The TWIC Pilot found that the increase in throughput delay resulting from a TWIC reader requirement is 2 seconds. Therefore, we do not believe a TWIC reader requirement at rail entrances to secure areas of Risk Group A facilities would lead to the results suggested by the commenters. While we seek to minimize the burdens associated with TWIC reader requirements, an exemption from such requirements at rail entrances would be inconsistent with the goal of the TWIC program to ensure that access to secure areas of the transportation system is limited to authorized individuals holding a TWIC.

One commenter suggested that TWIC-holders on all MTSA-regulated vessels and facilities should be required to visually display their TWICs, similar to the requirement at federally regulated airports. Another commenter opposed such a requirement, citing concerns that this practice might increase the number of lost TWICs.

In keeping with the longstanding tradition that seafarers keep their mariner credentials and other important documents on the bridge or stored in a secure place, this NPRM does not propose to require TWIC-holders to display their credentials at all times. Existing Coast Guard guidance acknowledges that such a requirement may not be practical in the marine environment.[70] Owners and operators are permitted to collect and store all crewmember TWICs in the vessel's pilot house or allow for TWICs to be stored in another secure location on board the vessel or at the facility.

*F. TWIC Reader Pilot Program*

This section discusses the background and findings of DHS's TWIC Pilot on TWIC reader functionality in the maritime sector. A copy of the TWIC Pilot report, as well as the GAO reports discussed below, are available for viewing in the public docket for this rulemaking. The Coast Guard seeks comments on the following characterizations of the TWIC Pilot, the Coast Guard's conclusions from the TWIC Pilot, and how the Coast Guard used the findings from the TWIC Pilot to inform the NPRM.

1. Background

The TWIC Pilot was established under Section 104 of the SAFE Port Act, and was designed to evaluate the business processes, technology, and operational impacts of implementing a TWIC reader system. The SAFE Port Act required the Secretary to conduct the TWIC Pilot at not fewer than five distinct geographic locations, and include vessels and facilities in a variety of environmental settings.[71] DHS conducted the TWIC Pilot in seven geographic locations, and covered five participant groups: (1) Container terminals; (2) large passenger vessels and terminals with more than 500 passengers; (3) break-bulk terminals; (4) petroleum facilities; and (5) small passenger vessels, towboats, and other facility types. DHS managed the TWIC Pilot through the joint participation of TSA and the Coast Guard, with grant funding provided by the Federal Emergency Management Administration through the Port Security Grant Program.

The TWIC Pilot consisted of three phases. In Phase 1 (Initial Technical Testing), DHS tested TWIC readers under controlled laboratory conditions to verify that the TWIC readers correctly processed biometric information from the TWIC, and could also perform other TWIC verification and validation operations in maritime environments.

In Phase 2 (Early Operational Assessment) DHS required pilot participants to install TWIC readers and begin using them. This phase allowed both TWIC-holders and security personnel to become familiar with TWIC readers and different operational modes. It also provided an opportunity to evaluate the initial technical performance of TWIC readers in maritime settings, and to address problems.

Phase 3 (System Test and Evaluation) required pilot participants to verify the identities of individuals granted unescorted access to secure areas based on potential requirements as set forth in the ANPRM. Data collected during Phase 3 included: (1) Impacts of the biometric verification process on vessel and facility operations; (2) measurement of wait times for access to secure areas; (3) TWIC reader and infrastructure failures and maintenance requirements; and (4) implementation and operating costs.

TSA completed data collection for the TWIC Pilot as of May 31, 2011. The SAFE Port Act required the Secretary to '' * * * submit a comprehensive report to the appropriate congressional committees * * * that includes: (A) The findings of the pilot program with respect to technical and operational impacts of implementing a transportation security card reader system; (B) any actions that may be necessary to ensure that all vessels and facilities * * * are able to comply with [TWIC reader] regulations; and (C) an analysis of the viability of equipment under the extreme weather conditions of the marine environment.'' DHS submitted the TWIC Pilot report to Congress on February 27, 2012.

2. General Findings

The TWIC Pilot noted a number of benefits associated with the use of TWIC readers. First, when used properly, TWIC readers provide an additional layer of security by reducing the risk that an unauthorized individual could gain access to a secure area. Owners and operators using TWIC readers can achieve this security risk reduction without significantly increasing throughput times at access points. Second, security is further enhanced by enabling owners and operators to assign access privileges to a specific, limited population of TWIC-holders. Finally, vessels and facilities using the TWIC as a site access token, in addition to as a means of identification, may benefit financially through the reduction of card management operational costs associated with identity vetting, card inventory, printing equipment, and issuance infrastructure.

The TWIC Pilot also elicited a number of operational challenges and lessons learned. Although the TWIC Pilot provided the most complete information available regarding the costs associated with large-scale TWIC reader implementation and integration for access control available, we note some limitations regarding the TWIC Pilot data. We were not able to obtain data from a statistically representative sample of the affected population of MTSA-regulated vessels and facilities affected by this proposed rule because the TWIC Pilot was a voluntary program. As such, it was necessary to extrapolate the findings of the TWIC Pilot across the entire affected population. There were also some variations as to how individual pilot participants reported their data to TSA, which made some data manipulations

[70] *See* Navigation and Vessel Inspection Circular (NVIC) No. 03–07, ''Guidance for the Implementation of the Transportation Worker Identification Credential (TWIC) Program in the Maritime Sector,'' (July 2, 2007).

[71] 46 U.S.C. 70105(k)(1)(B).

more difficult. Also, some of the cost reporting included costs that were not directly related to TWIC readers, but rather general physical security, and these were included in the pilot participants' cost estimates.

Additionally, while not all of the TWIC Pilot participants were in Risk Group A, using the costs associated with TWIC reader deployment at facilities not in Risk Group A does not adversely affect our overall estimates. Potential TWIC reader implementation costs should not differ greatly across risk groups, as the size and geography of a facility is independent of its risk grouping. The key difference between the risk groups is the potential consequences of a TSI at a particular facility, not the costs associated with potential TWIC reader deployment.

Since the passage of MTSA in 2002, the United States Government Accountability Office (GAO) has published a number of reports regarding implementation of the TWIC program, highlighting both progress and limitations. Copies of these reports are available for viewing on the GAO Web site at *www.gao.gov,* by clicking on the ''Reports & Testimonies'' tab, and using ''TWIC'' as your keyword search term, as well as in the docket. The GAO has conducted a review of the TWIC Pilot, highlighting some of the same limitations with respect to the quality of TWIC Pilot data we have described above. While we acknowledge that the TWIC Pilot contained certain data limitations, the TWIC Pilot provided the most detailed and wide-spread assessment of the impacts of deploying TWIC readers in the maritime sector to date. The TWIC Pilot provided useful data with respect to the costs associated with installing and integrating TWIC readers at facilities, as well as valuable TWIC-holder population data and TWIC reader failure rates, as experienced during the TWIC Pilot. As discussed below in Section III.H. ''Additional Data Sources,'' we supplemented TWIC Pilot data with other data sources as necessary to provide the most accurate estimates for cost and benefit possible. In accordance with 46 U.S.C. 70105(k)(3), the proposals in this NPRM are consistent with the findings of the TWIC Pilot.

The TWIC Pilot generally found that when TWIC readers are designed, installed, and operated in a manner consistent with the business considerations of the vessel or facility, they function properly. Conversely, the TWIC Pilot also noted a number of operational and technological difficulties that affected overall success at many pilot locations. The proposals in this NPRM are designed to be consistent with the findings of the TWIC Pilot.

3. Specific Challenges and Lessons Learned

The TWIC Pilot noted that processing delays at access points were sometimes compounded by user unfamiliarity with the TWIC authentication process. It is important to note that when a user is properly trained and acclimated to interface with the TWIC reader, transaction times decrease considerably. In this NPRM, we have included a 2-year compliance deadline for TWIC reader implementation to allow adequate time for proper training.

The TWIC Pilot noted that training requirements were often underestimated by TWIC Pilot participants. Additionally, TWIC-holders experienced challenges becoming familiar with different TWIC reader modes and processes. Switching among different TWIC reader modes complicated the learning process, impacting the efficiency of TWIC reader use. Additionally, TWIC-holders had difficulty interfacing with TWIC readers from multiple manufacturers with differing designs and user interfaces. Finally, some TWIC-holders presented the wrong finger, or did not hold their finger on the fingerprint sensor long enough to complete the transaction. These occurrences impeded operations and increased throughput times. In this NPRM, we have included a 2-year compliance deadline for TWIC reader implementation to allow adequate time for proper training.

The TWIC Pilot noted certain challenges that arose when using portable TWIC readers. At facilities where workers are required to enter and exit secure areas multiple times over short periods, it was particularly challenging to maintain biometric checks using portable readers. Additionally, some portable TWIC readers malfunctioned when used carelessly in wet conditions not aligned with vendor guidance. In this NPRM, we do not specifically require the use of portable TWIC readers. Instead, we take a flexible approach by allowing owners and operators to choose the type of TWIC readers that best suit their operational needs.

The TWIC Pilot noted that while some TWIC readers performed well throughout the TWIC Pilot, others were not as mature technologically or required adjustments. In one case, the TWIC readers repeatedly failed and had to be replaced by another vendor. We expect these challenges to be mitigated in the future because TSA is developing the QTL so that approved readers meet durability standards.

The TWIC Pilot noted that the ability of TWIC readers to work properly depends, in part, on a functioning TWIC card. In response, TSA established an Integrated Product Team (IPT) in conjunction with DHS that is continuing to review the nature and prevalence of non-functioning TWIC cards and seeking ways to resolve these technical issues.

The TWIC Pilot noted TWIC reader installation delays at some facilities where TWIC systems integrators were unfamiliar with other components of multi-functional systems. In this NPRM, we have included a 2-year compliance deadline for TWIC reader implementation to allow facilities and security personnel adequate time for proper training.

The TWIC Pilot noted challenges with respect to the registration of authorized TWIC-holders in a PACS. The registration process proved to be time-consuming. Some TWIC Pilot participants that were located within the same geographical region chose to operate using a regional registration database. This was a successful way to populate their various PACS. One factor that led to delays was the decision by some facilities to require TWIC-holders to enter their PIN as part of the registration process. Since many TWIC-holders rarely, if ever, used their PIN since activating their TWIC, some workers could not remember their PIN. These workers then had to visit a TWIC enrollment center to reset their PIN and return to the facility to complete the registration process. This NPRM does not propose to require facilities to register authorized TWIC-holders by requiring them to enter their PIN.

The TWIC Pilot noted that some participants failed to grant TWIC-holder rights to specific access points, which increased the number of invalid transactions using TWIC readers. Developing standard operating procedures to assign access privileges should mitigate this issue.

The TWIC Pilot noted that TWIC reader system architecture played a significant role in overall technical efficiency, performance, and throughput times. The TWIC Pilot participant with a dedicated network only used by TWIC readers and PACS showed faster transaction times, higher validation rates, and fewer technical issues than other TWIC Pilot participants. System configurations that used hard wired networks were more efficient with respect to network speed and availability than wireless networks. Systems that included TWIC readers

within the security architecture encountered fewer operational issues. Finally, TWIC reader implementation costs were lower if facilities were able to use existing infrastructure. We encourage the regulated population to take note of these lessons learned. Additionally, in this NPRM, we take a flexible approach by allowing owners and operators to choose the type of TWIC readers that best suit their operational needs.

The TWIC Pilot found that a consistent experience on the part of TWIC-holders and security personnel enhanced the efficiency of TWIC reader use. TWIC-holders who reported to the same facility on a daily basis had a consistent user experience and learned to interface with TWIC readers quickly. TWIC-holders whose work required them to access multiple facilities, however, experienced challenges becoming familiar with TWIC readers from several manufacturers with different designs and interfaces, as well as many site-specific business processes and requirements. Different TWIC reader ergonomics found at different access points further compounded these challenges. For example, truck drivers visiting several facilities encountered TWIC readers that were sometimes placed at awkward heights or distances, making the readers difficult to reach.

The TWIC Pilot tested both fixed and portable TWIC readers in different modes of operation. In contactless mode, the card is scanned by holding it within 4 inches of the TWIC reader. In contact mode, the card must be inserted into a slot that allows direct contact between the TWIC reader and the chip embedded in the TWIC. The TWIC Pilot found that when contactless TWIC readers are used in a non-biometric mode to verify that the card is authentic, has not expired, and is not on the CCL, and in a manner consistent with their intended environment, access point throughput times were less than throughput times required to visually inspect TWICs. When used in non-biometric mode, however, it is also necessary to visually compare the photograph on the TWIC to the TWIC-holder. Although adding a biometric match to the above TWIC reader functions may take slightly longer than mere visual inspection, the TWIC Pilot did not find that the resulting access point throughput delays impacted business operations. Nonetheless, using TWIC readers in the biometric mode significantly increases the assurance that only TWIC-holders are permitted to access secure areas.

The TWIC Pilot also found that fixed readers with both contact and contactless interfaces yielded a higher validation rate than fixed readers that only used the contactless interface to read the TWIC. A contact read required the TWIC to be inserted into the contact slot of the TWIC reader, which reduced the potential for incorrectly placing the TWIC, and provided an alternative to the TWIC's internal antennae.

A successful contactless read requires the user to hold the card motionless on or near the surface of the TWIC reader for approximately 2 seconds, which was not initially understood by many pilot participants. As a remedial measure, the posting of explanatory diagrams helped overcome this problem. The TWIC Pilot found that switching between different TWIC reader modes created a confusing process for TWIC-holders and had a negative impact on the efficiency of TWIC reader use.

Accordingly, the proposals in this NPRM enable owners and operators to use fixed or portable, contact or contactless TWIC readers in a single mode of operation as much as possible. Each owner or operator would have the discretion to configure a system that best suits the vessel or facility.

The TWIC Pilot found that facilities with an existing PACS that could be easily adapted to incorporate TWIC reader technology took less time to install than facilities without that existing infrastructure. Consistent with that finding, this NPRM allows for the integration of TWIC reader technology into an existing PACS.

The TWIC Pilot found that geographic location did not affect the efficiency of TWIC reader functionality. The TWIC Pilot found, however, that at varying locations, some TWIC readers experienced difficulty scanning fingerprints in inclement weather. Fully encapsulated fixed contactless TWIC readers withstood harsh weather, whereas contact TWIC readers, and TWIC readers exposed to the elements were sensitive to inclement weather conditions. Throughout the TWIC Pilot, the conditions under which TWIC readers had to perform were significantly more challenging than those commonly found at entrances to office buildings and other more controlled locations and environments. The TWIC Pilot demonstrated that TWIC readers installed in harsh environments will occasionally be contaminated with debris, and a maintenance program to perform regular inspections and cleaning cycles is necessary. The TWIC Pilot noted, however, that most of the challenges associated with weather can be overcome with proper planning that takes environmental conditions into consideration. Proper planning means that a facility's business practices will be useful in determining which type of TWIC readers and accompanying infrastructure to use. For example, if an access point is exposed to direct sunlight, the facility can mitigate glare by using an awning or hood. If an access point is exposed to harsh weather, the facility may wish to use an encapsulated fixed TWIC reader or instead use a portable TWIC reader that is kept inside a nearby security guard booth.

TSA is developing the QTL so that approved readers meet durability standards. Additionally, in this NPRM, we're proposing requirements that provide owners and operators the flexibility to choose the TWIC reader that best suits their operational needs.

*G. HSI Report*

This section summarizes the analysis and recommendations provided by HSI after evaluating the risk-based approach that formed the basis of the proposals in the ANPRM. A non-SSI version of the HSI Report is available for viewing in the public docket for this rulemaking.

Prior to publishing the ANPRM, we developed a risk-based approach based on MSRAM, to inform our proposals for more stringent TWIC reader requirements on higher-risk vessels and facilities. We engaged HSI to obtain an independent peer review of our analysis. HSI is a federally funded research and development center established by the Secretary, pursuant to Section 312 of the Homeland Security Act of 2002 (Pub. L. 107–296). On October 21, 2008, HSI issued a final report, titled ''Independent Verification and Validation of Development of Transportation Worker Identification Credential (TWIC) Reader Requirements'' (HSI Report). The HSI Report provided information and recommendations that were useful in formulating the proposals in this NPRM.

The HSI Report verifies that our AHP/MSRAM analysis matches the way we described it, and that its findings can be reproduced. The HSI Report also validates that our AHP/MSRAM analysis is technically sound. While the HSI Report suggests that some adjustments to the results of our analysis might be necessary, the report concludes that our methodology is appropriate for establishing the risk ranking of vessels and facilities set forth in the ANPRM.

The HSI Report notes that Risk Group A is well defined, but the distinction between Risk Groups B and C is not as clear. The HSI Report also notes that, while adjustments could be suggested with respect to the ANPRM's proposed

TWIC reader requirements, the overall risk-based approach to specifying the TWIC reader requirements is fundamentally sound. The HSI Report recommends that we consider further analysis of how to best group vessels and facilities into appropriate risk-based categories.

Our proposals in this NPRM are consistent with the above conclusions and recommendations. Whereas the ANPRM proposed different TWIC requirements for Risk Groups B and C, this NPRM proposes the same TWIC requirements for both of those risk groups. We expect to continue analyzing the risk rankings to determine whether alternative or additional considerations would yield more appropriate risk groupings and corresponding TWIC requirements. As noted earlier, if the Coast Guard changes the risk groupings, it will be done through rulemaking and the public will have an opportunity to comment.

The HSI Report also recommends that we consider better defining the concept of TWIC utility. As used in the context of the AHP/MSRAM analysis, TWIC utility accounts for the reduced risk to a vessel or facility due to TWIC implementation. The HSI Report acknowledges that a clearer definition of this concept may require analysis of each individual vessel and facility, which would substantially expand the scope of the process of developing TWIC reader requirements. The HSI Report suggests that we consider an approach that combines general analyses of broad risk groups with specific analyses of individual vessels and facilities. We are considering the feasibility of implementing this recommendation.

The HSI Report recommends that we consider adding flexibility to TWIC reader requirements by providing a process through which owners and operators may seek a waiver of TWIC reader requirements based on the unique features of a specific vessel or facility. The rationale for this recommendation is that while TWIC reader requirements apply to an entire risk group, each risk group is comprised of a range of types of vessels and facilities with fundamentally different security systems. In response to this recommendation, we note that waiver provisions already exist in current 33 CFR 104.130, 105.130, and 106.125. These provisions enable an owner or operator to apply for a waiver of any requirement that the owner or operator considers unnecessary in light of the nature or operating conditions of a vessel or facility.

The HSI Report recommends that we consider using dynamic consequence data instead of the static maximum consequence data currently used as part of the MSRAM analysis. The rationale for this recommendation is that maximum consequence would necessarily change depending on how vessels and facilities are used. For example, a cruise ship terminal would have a different maximum consequence when cruise ships are docked at the facility, as opposed to when the port is empty. We believe that, due to the amount and complexity of dynamic consequence data, obtaining such data would not be feasible. Furthermore, use of dynamic consequence data would eliminate or at least dramatically reduce the predictability of regulatory requirements, and would likely not reduce costs significantly, as most costs would be borne anyway. Nonetheless, we are considering the feasibility of implementing this recommendation.

*H. Additional Data Sources*

TWIC Pilot data was supplemented with other data sources as necessary to provide the most accurate estimates for cost and benefit possible. Other data sources included the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database for population figures, MSRAM for risk hierarchy and consequence data, the General Services Administration schedule for TWIC reader hardware and software costs, Environmental Protection Agency data for estimates for truck throughput, and contracted studies for general discussion points on access control systems. For a more detailed discussion on the use of this data, please refer to the ''Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis,'' which is available in the public docket for this rulemaking. The Coast Guard seeks public comment on whether or not there are additional data sources that should be considered. If there are, please include information in your comments about these data sources and the reason for their relevance.

*I. Advisory Committee Input*

This section discusses the input we received from advisory committees in connection with this rulemaking.

The Coast Guard has a long tradition of consulting with its advisory committees before taking regulatory action. We acknowledge the benefit of consulting with advisory committees. Prior to issuing the ANPRM, we sent a task statement to MERPAC, NMSAC, and TSAC, asking 18 questions related to TWIC reader requirements. This task statement is available for viewing in the public docket for this rulemaking. We accepted and incorporated a number of the advisory committee recommendations into the ANPRM and this NPRM. For example, we incorporated TSAC's recommendation to set the crew size cutoff number at 14 for determining when to exempt vessels from TWIC reader requirements as discussed more fully below in Section IV.E. ''TWIC Reader Exemption for Vessels With 14 or Fewer TWIC-holding Crewmembers.'' Both NMSAC and MERPAC recommended that we wait for completion of the TWIC Pilot before publishing an NPRM on TWIC reader requirements. MERPAC recommended against requiring owners and operators to verify TWIC-holder PIN information. MERPAC also recommended that low risk vessels and facilities should not be subject to TWIC reader requirements. These are some examples of the advisory committee recommendations we incorporated into this NPRM. We greatly appreciate advisory committee input into this program. Copies of each advisory committee's formal recommendations and responses to the task statement are available for viewing in the public docket for this rulemaking.

## IV. Section-by-Section Description of Proposed Rule

This section provides a discussion of the regulations we propose in this NPRM, which include: updated definitions relevant to this rulemaking; a provision on the Federalism issues associated with the Coast Guard's maritime security regulations; TWIC reader and inspection requirements for Risk Groups A, B, and C, applicable in both normal and special circumstances; deadlines for compliance with the proposed regulatory requirements; TWIC reader recordkeeping requirements; TWIC-related risk group classifications for vessels and facilities; requirements for the physical placement of TWIC readers; and several technical amendments to the regulations.

We note that, if finalized, the proposed regulations would be subject to the control and compliance measures in 33 CFR 101.410, which give the COTP authority to impose measures to rectify non-compliance. The proposed regulations would also be subject to the relevant civil and/or criminal penalties in 33 CFR 101.415 for violations of any provision in 33 CFR subchapter H.

*A. Definitions*

We propose to amend 33 CFR 101.105 by adding several new defined terms.

The term ''biometric match'' would mean a confirmation that: one of the two

biometric (fingerprint) templates stored in the TWIC matches the scanned fingerprint of the person presenting the TWIC; or the alternate biometric stored in a PACS matches the corresponding biometric of the person.

The term ''Canceled Card List (CCL)'' would mean the list of TWIC Federal Agency Smart Credential-Numbers that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or because the card has been reported lost, stolen, or damaged.

The term ''card authentication'' would mean the electronic verification that the card presented is a valid TWIC issued by TSA.

The term ''Card Holder Unique Identifier (CHUID)'' would mean the standardized data object comprised of the FASC–N, globally unique identifier, expiration date, and certificate used to validate the data integrity of other data objects on the credential.

The term ''card validity check'' would mean the verification that a TWIC has not been revoked or expired.

The term ''Mobile Offshore Drilling Unit (MODU)'' is defined by reference to 33 CFR 140.25.

The term ''Offshore Supply Vessel (OSV)'' is defined by reference to 46 CFR 125.160.

The term ''Physical Access Control System (PACS)'' would mean a system that includes devices, personnel, and policies that controls the access to and within a facility or vessel.

The term ''Risk Group'' would mean the risk ranking assigned to a vessel, facility, or OCS facility for the purpose of TWIC requirements.

The term ''TWIC reader'' would mean an electronic device used to verify and validate: the authenticity of a TWIC; the identity of the TWIC-holder as the legitimate bearer of the credential; that the TWIC is not expired; and that the TWIC is not on the CCL. The term is specifically defined by reference to TSA's Qualified Technology List of acceptable TWIC readers, because only those devices meet TSA's required specifications.

We propose to amend 33 CFR 101.105 by deleting the term ''recurring unescorted access''. This term was included in 33 CFR 101.105 as part of the TWIC 1 final rule, though we determined at that time to defer implementing TWIC reader requirements. RUA was initially proposed to provide relief to owners and operators of vessels otherwise required to use TWIC readers, because of the familiarity that exists between a relatively small number of crewmembers. Two important changes in approach from the ANPRM to this NPRM render RUA an unnecessary provision. First, this NPRM proposes to exempt from TWIC reader requirements all vessels with 14 or fewer TWIC-holding crewmembers, based on the SAFE Port Act's provision that prohibits requiring TWIC readers on vessels that the Secretary has determined do not have the requisite number of TWIC-holders as crewmembers.[72] This exemption provides relief equivalent to that which RUA would have provided. Second, whereas the ANPRM proposed to require TWIC readers for Risk Groups A and B, this NPRM proposes to require TWIC readers for Risk Group A only. This change reduces the number of vessels and facilities to which TWIC reader requirements would apply, and renders the need for RUA as a mechanism for regulatory relief unnecessary.

*B. Federalism*

A Presidential Memorandum, dated May 20, 2009, entitled ''Preemption,''[73] requires an agency to codify a preemption provision in its regulations if the agency intends to preempt State law. We propose to add new 33 CFR 101.112, providing a statement regarding the preemption principles that apply to 33 CFR subchapter H.

We believe the field-preemption Federalism principles articulated in *United States* v. *Locke* and *Intertanko* v. *Locke*[74] apply to 33 CFR parts 101, 103, 104, and 106. Therefore, States and local governments are foreclosed from regulating within this field. We believe the Federalism principles articulated in *Locke* also apply to 33 CFR part 105, at least insofar as a State or local law or regulation applicable to MTSA-regulated facilities for the purpose of their protection, would conflict with a Federal regulation (i.e., it would either actually conflict or would frustrate an overriding Federal need for uniformity).

*C. Additional Persons Required To Obtain TWICs*

This NPRM withdraws the ANPRM's proposal to include non-credentialed individuals engaged on towing vessels not regulated under 33 CFR part 104 among the list of mariners required to possess a TWIC. We seek public comment on the number of vessels pilots without a Federal license, and whether a specific provision to include them in the regulatory requirement to obtain a TWIC is necessary.

In the ANPRM, we proposed to explicitly require non-Federally licensed vessel pilots and non-credentialed individuals engaged on towing vessels not regulated under 33 CFR part 104 to possess a TWIC. The purpose of this proposal was to update the regulations to more thoroughly incorporate the list of individuals required by 46 U.S.C. 70105(b) to possess a TWIC.

Subsequent developments have caused us to withdraw part of the ANPRM's proposal. Section 809 of the CGAA 2010 authorized the Secretary to exempt any credentialed mariner who is not granted unescorted access to secure areas of a vessel from the requirement to possess a TWIC. On December 19, 2011, the Coast Guard's Office of Vessel Activities (CG–543) published Policy Letter No. 11–15,[75] describing both policy and forthcoming regulatory solutions that we are undertaking to implement Section 809. Policy Letter No. 11–15 contains exemptions for certain mariners from the requirement to obtain or hold a TWIC. Exempt mariners would include mariners not operating under the authority of a credential and mariners serving on a vessel not required to have a Vessel Security Plan. These are mariners that the ANPRM's proposal would have explicitly included among the list of mariners required to obtain a TWIC.

In light of Section 809 and related Coast Guard regulatory action, this NPRM withdraws the ANPRM's proposal to include non-credentialed individuals engaged on towing vessels not regulated under 33 CFR part 104 among the list of mariners required to possess a TWIC. Additionally, while there may be some vessel pilots that do not hold Federal licenses, we have not determined whether there is a population of State-licensed vessel pilots that are not otherwise required to obtain a TWIC because they access secure areas of MTSA-regulated vessels. We seek public comment on this subject, and whether a specific provision to include them in the regulatory requirement to obtain a TWIC is necessary. If there is a population of State-licensed vessel pilots not covered under the current regulatory requirement to obtain a TWIC, we intend to revise 33 CFR 101.514 to cover that population.

[72] 46 U.S.C. 70105(m)(1).

[73] 74 FR 24693.

[74] 529 U.S. 89, 120 S.Ct. 1135 (March 6, 2000).

[75] CG–543 Policy Letter No. 11–15, ''Processing of Merchant Mariner Credentials (MMC) For Mariners Not Requiring a Transportation Worker Identification Credential,'' available for viewing at *https://homeport.uscg.mil/*.

*D. TWIC Reader Requirements for Risk Group A*

We propose to add new 33 CFR 101.520 that sets forth the TWIC reader requirements for Risk Group A. We have determined that owners and operators of vessels or facilities in Risk Group A should be required to implement the TWIC's most protective measures using a TWIC reader or TWIC-integrated PACS.

At MARSEC Level 1, all persons seeking unescorted access to secure areas would be required to present a TWIC and fingerprint for biometric identity verification, card authentication, and card validity check. The owner or operator would be required to perform the card validity check based on CCL information no more than 7 days old. The owner or operator may perform these functions using a TWIC reader or a TWIC-integrated PACS. If using a PACS, biometrics other than fingerprints may be used to perform the identity verification, provided that the owner or operator links the person, the TWIC, and the alternate biometric in the PACS. To do this, the owner or operator would be required to perform a one-time biometric match and card authentication using a TWIC reader. Owners or operators would be required to explain in their security plans how the PACS performs the required security functions and how the SSI captured by the PACS is protected.

At MARSEC Level 2, the same procedures would apply as those at MARSEC Level 1, except that the owner or operator would be required to perform the card validity check based on CCL information no more than 1 day old. The heightened security threats present at elevated MARSEC Levels justify this additional requirement.

We propose two additional provisions in 33 CFR 101.520 to ensure that CCL information is updated and used appropriately. First, owners and operators would be required to update CCL information within 12 hours of any increase in MARSEC Level, regardless of when the CCL information was last updated. Second, owners and operators would be required to use the most recently obtained CCL information when conducting card validity checks.

Finally, we propose a provision in 33 CFR 101.520 that would authorize the COTP to temporarily suspend TWIC reader requirements at a facility if the COTP determines that such requirements are causing delays resulting in excessive vehicle build-up or other unintended consequence. A facility owner or operator could contact the COTP seeking such a determination. During the period of any such suspension, the owner or operator would be required to perform visual TWIC inspections for identity verification, card authentication, and card validation.

*E. TWIC Reader Exemption for Vessels With 14 or Fewer TWIC-Holding Crewmembers*

We propose to add new 33 CFR 101.520(e), exempting all vessels with 14 or fewer TWIC-holding crewmembers from TWIC reader requirements. The statutory basis for this exemption is the SAFE Port Act provision that prohibits the Secretary from requiring TWIC readers on a vessel unless the vessel has more individuals on the crew required to have a TWIC than the number the Secretary determines warrants such a reader.[76] The underlying rationale for this exemption is that vessels with a small enough number of TWIC-holders on board have a reduced TSI vulnerability from unauthorized access because the small number of crewmembers are easily recognizable and known to one another. We propose 14 as the cutoff number based on a recommendation from TSAC. According to TSAC, vessels with 14 or fewer crewmembers have a reduced vulnerability because the individuals are all ''known'' to one another. The number was developed by taking into account the fact that for a small vessel, such as a towing vessel or offshore supply vessel, the crew would typically include up to one Master, one Chief Engineer, and three four-person crews who rotate through watch shifts.

We seek public comment on this proposal to exempt all vessels with 14 or fewer TWIC-holding crewmembers from TWIC reader requirements, including whether 14 is an appropriate cut-off number. We request that commenters please explain and provide available data to support their comments.

We recognize that, particularly for smaller vessels such as towing vessels, the value of electronic identity verification is less than it is for facilities, which generally interact with greater numbers of vendors, visitors, and facility employees. For this reason, and because TWIC readers are only proposed for Risk Group A, we believe it is neither appropriate nor necessary to exempt facilities with 14 or fewer TWIC-holders from TWIC reader requirements.

[76] 46 U.S.C. 70105(m).

*F. TWIC Inspection Requirements for Risk Groups B and C*

We propose to add new 33 CFR 101.525 and 101.530 that set forth the TWIC visual inspection requirements for Risk Groups B and C, respectively. In this NPRM, we are not proposing TWIC reader requirements for vessels and facilities in Risk Groups B and C. We believe the overall approach in this proposed rule would implement the TWIC reader program in a targeted manner that enhances the security of MTSA-regulated vessels and facilities without imposing undue burdens. We request public comment on this determination.

At all MARSEC Levels, all persons seeking unescorted access to secure areas of vessels or facilities in Risk Groups B or C would be required to present a TWIC for visual identity verification, card authentication, and card validity check, prior to each entry. An owner or operator would perform identity verification by visually matching the photograph on the TWIC to the individual presenting it. An owner or operator would verify TWIC authenticity by visually checking its security features to determine whether it has been tampered with or forged. An owner or operator would validate the TWIC by visually checking the expiration date on the face of the TWIC to determine whether it has expired. Owners and operators of vessels or facilities in Risk Groups B and C would not be required to check TWICs against the CCL.

As discussed above in Sections II. and III. above, we are considering a phased approach to implementing TWIC reader requirements by proposing such requirements first for vessels and facilities in Risk Group A, where the risk of harm is greatest. We have estimated that for Risk Group A, the ratio of annualized cost of TWIC reader requirements to average consequence figures (the monetized costs of fatalities and injuries resulting from a TSI) warrants the TWIC reader requirements proposed in this NPRM. For Risk Group B, we believe the estimated ratio of annualized cost of TWIC reader requirements to average consequence figures supports our phased approach. We will continue to analyze risk data and consider whether additional or modified TWIC reader requirements would be warranted in the future. For a more detailed discussion of the costs and benefits of the proposals in this NPRM, please refer to Section V., ''Regulatory Analyses'' below.

The proposed TWIC inspection requirements in 33 CFR 101.525 and

101.530 would be minimum requirements. We have included proposed regulatory provisions stating that owners and operators would have the discretion to impose access control measures that are stricter than the minimum regulatory requirements.

Although this NPRM proposes the same substantive TWIC inspection requirements for Risk Groups B and C, these requirements appear in separate sections because we are continuing to gather data and analyze whether different requirements would be appropriate for these risk groups. Any such modifications would be proposed in a separate rulemaking document, with the opportunity provided for public comment.

*G. TWIC Inspection Requirements in Special Circumstances*

We propose to add new 33 CFR 101.535 that sets forth TWIC inspection requirements in special circumstances. These provisions are designed to provide an appropriate level of flexibility in the TWIC reader and inspection requirements when special circumstances arise.

If an individual is unable to present a TWIC because it has been lost, damaged, or stolen, and the individual has previously been granted unescorted access to secure areas and is known to have previously possessed a TWIC, an owner or operator would be permitted to grant the individual unescorted access to secure areas for a period of no longer than 7 consecutive days, provided that the following conditions are met: (1) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f); (2) the individual presents another identification credential that meets the requirements of 33 CFR 101.515; and (3) there are no other suspicious circumstances associated with the individual's claim of loss or theft. With the exception of these individuals, all others who are granted unescorted access to secure areas would be required to produce their TWIC upon request from TSA, the Coast Guard, any other authorized DHS representative, or a law enforcement officer.

If an individual cannot present a TWIC for any reason other than those outlined in the immediately preceding paragraph, the individual may not be granted unescorted access to secure areas. In order to access secure areas, the individual would need to be escorted by a TWIC-holder authorized to be in the secure area.

In some instances, when an individual has poor quality fingerprints, a TWIC reader may not be able to consistently perform the biometric identity verification function. Also, a small number of TWICs will be issued that contain either poor quality fingerprint templates, mostly due to badly damaged fingers, or no fingerprint minutiae, in the case of amputations. We expect owners and operators to describe the exception handling process to be used in such cases in their security plans. The exception handling process may include granting unescorted access after the individual has successfully provided a PIN. Alternatively, an owner or operator may require the individual to present an alternative biometric, such as a retina scan or other biometric that has been incorporated into a PACS.[77]

If a TWIC reader malfunctions, an owner or operator would still be permitted to grant the individual unescorted access to secure areas, provided that certain conditions are met. First, the individual would be required to have previously been granted unescorted access to secure areas in the past, and the individual would be required to be known to have a TWIC. Second, the owner or operator would be required to perform identity verification, card validation and card authentication by visual inspection. An owner or operator may rely on this alternative for a period of 7 calendar days while the TWIC reader malfunction is corrected.

TWIC requirements in 33 CFR 104.265, 105.255, and 106.260 currently contain provisions regarding disciplinary measures to prevent fraud and abuse, coordination of access control with other vessels and conveyances, and security plan requirements. We propose to relocate those provisions to 33 CFR 101.535(f)-(h).

*H. Compliance Deadlines*

We propose to amend 33 CFR 104.115 and 105.115 to set forth the required compliance deadlines with respect to TWIC reader requirements. Within 2 years after publication of the TWIC reader final rule, owners and operators would be required to be operating in accordance with the requirements contained in that final rule. Also, within 2 years after publication of the TWIC reader final rule, owners and operators would have to amend their security plans to indicate how they implement the TWIC reader requirements contained in the applicable sections of 33 CFR parts 101, 104, and 105.

[77] Section 814 of the CGAA 2010 allows the Secretary to use a secondary authentication system to verify the identification of individuals using TWIC when the individual's fingerprints are not able to be taken or read.

In the ANPRM, we were not proposing to amend the section on ASPs to require amendments within 2 years of the final rule. Instead, in the ANPRM, we said we would exercise our authority under 33 CFR 101.120(d)(1)(ii) to require those entities using ASPs to amend them to incorporate TWIC requirements. For the purpose of consistency with the other vessels and facilities subject to 33 CFR parts 104, 105, and 106, this NPRM eliminates the ANPRM's proposed approach to treat entities with approved ASPs differently. Accordingly, this NPRM proposes to require entities to update their ASPs in the same manner and on the same schedule as the other vessels and facilities subject to 33 CFR parts 104, 105, and 106.

We recognize that in addition to this NPRM, there are a number of ongoing Coast Guard rulemakings (e.g., *Updates to 33 CFR Subchapter H: Maritime Security* (RIN 1625–AB30) and *Consolidated Cruise Ship Security Measures* (RIN 1625–AB38)) that could affect vessel, facility, and OCS facility security plans in the near future. In 2011, a majority of facilities that would be subject to these proposed requirements already updated and submitted for approval security plans in accordance with 33 CFR subchapter H. If each of the ongoing rulemaking projects required an update to security plans, there could be a significant increase in workload for owners and operators, as well as at the Coast Guard Marine Safety Center, Districts, and Sectors. We are currently examining several options to coordinate the rulemakings and manage the plan submission and re-approval process to ensure that plan changes occur only as often as necessary to incorporate any new regulatory requirements. While this NPRM proposes a 2-year deadline for updated security plans, we invite comments or suggestions from the public on how to streamline and reduce the level of effort for all stakeholders.

*I. Recordkeeping*

We propose to amend 33 CFR 104.235 and 105.225 to set forth TWIC reader recordkeeping requirements. These recordkeeping requirements would apply when TWIC readers are used, and not in the special circumstances described in the proposed regulations when the owner or operator is permitted to rely on visual TWIC inspection. Owners and operators using TWIC readers, with or without a PACS, would be required to maintain certain records for at least 2 years. During that time, owners and operators would be required to make those records available to the

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

*J. Risk Group Classifications*

We propose to add new 33 CFR 104.263, 105.253, and 106.258 to set forth the risk group classifications for vessels and facilities. The risk group classifications proposed in the NPRM are the same as those proposed in the ANPRM, with minor technical changes, as follows:

For vessels subject to 33 CFR part 104, this NPRM proposes the following risk group classifications:

Risk Group A

(1) Vessels that carry Certain Dangerous Cargoes (CDC) in bulk.

(2) Vessels certificated to carry more than 1,000 passengers.

(3) Towing vessels engaged in towing a barge or barges subject to (1) of this section or vessels subject to (2) of this section.

Risk Group B

(1) Vessels that carry hazardous materials other than CDC in bulk.

(2) Vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues.

(3) Vessels certificated to carry 500 to 1,000 passengers.

(4) Towing vessels engaged in towing a barge or barges subject to (1), (2), or vessels subject to (3) of this section.

Risk Group C

(1) Vessels carrying non-hazardous cargoes that are required to have a vessel security plan (VSP).

(2) Vessels certificated to carry less than 500 passengers.

(3) Towing vessels engaged in towing a barge or barges subject to (1) of this section or vessels subject to (2) of this section.

(4) Mobile Offshore Drilling Units (MODUs).

(5) Offshore Supply Vessels (OSVs) subject to 46 CFR chapter I, subchapter L or I.

For facilities subject to 33 CFR part 105, this NPRM proposes the following risk group classifications:

Risk Group A

(1) Facilities that handle Certain Dangerous Cargoes (CDC) in bulk.

(2) Facilities that receive vessels certificated to carry more than 1,000 passengers.

(3) Barge fleeting facilities that receive barges carrying CDC in bulk.

Risk Group B

(1) Facilities that receive vessels that carry hazardous materials other than CDC in bulk.

(2) Facilities that receive vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues.

(3) Facilities that receive vessels certificated to carry 500 to 1,000 passengers.

(4) Facilities that receive towing vessels engaged in towing a barge or barges carrying hazardous materials other than CDC in bulk, crude oil, or towing vessels certificated to carry 500 to 1,000 passengers.

Risk Group C

(1) Facilities that receive vessels carrying non-hazardous cargoes not otherwise included in Risk Groups A or B.

(2) Facilities that receive vessels certificated to carry less than 500 passengers.

(3) Facilities that receive towing vessels engaged in towing a barge carrying non-hazardous cargoes or less than 500 passengers.

This NPRM proposes to classify all OCS facilities subject to 33 CFR part 106 into Risk Group B.

As discussed more fully above in Section III.C., we used the AHP to conduct a risk-based analysis of MTSA-regulated vessels and facilities. We identified 68 distinct types of vessels and facilities based on their purpose or operational description. We then assessed each of the 68 types of vessels and facilities using three factors: (1) Maximum consequences to that vessel or facility resulting from a terrorist attack; (2) criticality to the nation's health, economy, and national security; and (3) utility of the TWIC in reducing risk.

For the first factor, we used the Coast Guard's MSRAM terrorism risk-analysis tool to calculate the maximum potential consequence resulting from the total loss of a target, factoring in injury and loss of life, economic and environmental impact, symbolic effect, and national security impact. We averaged these MSRAM consequences within each of the 68 types to develop a standard consequence for each type.

For the second and third factors, we considered the impact of the total loss of a vessel or facility beyond the immediate local consequences, and the utility of the TWIC program in reducing a vessel or facility's vulnerability to a terrorist attack.

Using the AHP, we combined the above three factors and developed an overall risk ranking of vessels and facilities by type. At the end of this process, types of vessels and facilities with similar scores were combined into one of three risk groups. This NPRM proposes to classify vessels and facilities into Risk Groups A, B, and C based on the AHP risk rankings.

Upon further analysis of the data generated through the AHP process, we note that certain types of facilities currently categorized in Risk Group B have relatively high MSRAM consequence scores. These facilities include petroleum refineries,[78] non-CDC bulk hazardous materials facilities, and petroleum storage facilities. Due to their high MSRAM consequence scores, we are considering whether TWIC reader requirements would be appropriate for these three types of facilities and to include these types of facilities into Risk Group A. Note, however, that despite the relatively high consequence scores for these three facility types, they do not handle CDC in bulk. Like all Risk Group B facilities, these three facility types pose less operational risk than Risk Group A facilities because they do not handle CDC in bulk. We are soliciting public comments on this issue. Specifically, we request public comments on whether any or all of petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities should be categorized in Risk Group A. We also seek public comments on how to define these facilities for the purpose of this rulemaking. Please see Section V., ''Regulatory Analyses'' below for a discussion of the costs and benefits associated with this alternative.

*K. Movement Between Risk Groups*

We propose to add 33 CFR 104.263(d) and 105.253(d) to address the movement between risk groups by vessels and

[78] Note that Risk Group A, as currently proposed in the NPRM, captures certain petroleum refineries. In the NPRM, Risk Group A includes refineries that handle Certain Dangerous Cargoes (CDCs) in bulk or receive vessels that do the same. There are 16 such refineries.

facilities, based on the materials they are carrying or handling, or the types of vessels they are receiving at any given time. These regulatory provisions are designed to provide flexibility to owners and operators of vessels and facilities that only meet the Risk Group A criteria on a periodic basis. These provisions are not mandatory. The owner or operator of such a vessel or facility could choose to maintain its Risk Group A status, even during those periods when the vessel or facility is not handling or carrying materials that meet the Risk Group A criteria. However an owner or operator wishing to take advantage of one of these provisions would be required to explain how the vessel or facility would move between risk groups in an amended security plan. The security plan would be required to account for the timing of such movement, as well as how the owner or operator would comply with the requirements of the higher- and lower-level risk groups, with particular attention to the security measures to be taken when moving from a lower-level risk group to a higher-level risk group.

*L. Physical Placement of TWIC Readers*

We propose to amend 33 CFR 104.265(a)(4) by requiring a vessel owner or operator to place TWIC readers at the vessel's access points only, regardless of whether the secure area encompasses the entire vessel. Thus, even if the secure area does not encompass the entire vessel (e.g., a passenger vessel consisting of secure areas and passenger and employee access areas), TWIC readers would be required only at the points of access to the vessel itself. TWIC-holders may be granted unescorted access to the vessel's secure areas after the TWIC has been verified, validated, and authenticated at a vessel access point. TWIC-holders may then move from passenger/employee access areas to secure areas without processing through a TWIC reader each time.

We propose to amend 33 CFR 105.255(a)(4) by requiring a facility owner or operator to place TWIC readers at the access points to a facility's secure areas. If the entire facility is designated as a secure area, then TWIC readers would be required only at the facility's access points. If the secure area does not encompass the entire facility, then TWIC readers would be required at access points to the secure areas.

We request additional comments from the public on the proposed regulatory provisions regarding the placement of TWIC readers for vessels and facilities.

*M. Technical Amendments*

We propose several technical amendments to remove references to dates no longer relevant and to add or change cross-references within the regulations to align with the proposed new or updated provisions. These amendments appear at 33 CFR 101.514, 101.515(d)(2), 104.105(d), 104.115(c), 104.200(b), 104.260(d)(1), 104.265(d)(1), 104.265(e)(8), 104.265(f)(11), 104.267(a), 104.292(b), 104.292(e), 104.405(a)–(b), 105.110(b), 105.115(c)–(d), 105.200(b), 105.255(d)(1), 105.255(e)(8), 105.255(f)(10), 105.257(a), 105.290(b), 105.296(a)(4), 105.405(a)–(b), 106.110(d)–(e), 106.200(b), 106.260(d)(1), 106.260(e)(5), 106.260(f)(9), 106.262(a), and 106.405(a)–(b).

*N. Privacy*

When an individual's TWIC is scanned using a TWIC reader, the TWIC reader captures limited information, including the TWIC-holder's FASC–N as well as the date and time of the scan. The TWIC-holder's name would also be captured in limited circumstances, depending on the type of TWIC reader employed. For example, a TWIC reader only captures the TWIC-holder's name when operating in ''contact'' mode,[79] and only after the TWIC-holder enters a 6–8 digit PIN.[80] An integrated PACS may also capture the name of the TWIC-holder.

The proposed rule contains recordkeeping requirements for owners or operators using TWIC readers. Owners and operators using TWIC readers, with or without a PACS, would be required to maintain certain records for at least 2 years. During that time, owners and operators would be required to make those records available to the Coast Guard upon request. Those records include, with respect to each individual granted unescorted access to a secure area: (1) FASC–N; (2) date that access was granted; (3) time that access was granted; and (4) if captured, the name of the individual to whom access was granted.

If a TWIC reader or PACS captures the required data when the TWIC is scanned, and can retain and reproduce that data, the recordkeeping requirement would be met. Owners and operators would also be required to maintain records to demonstrate that they have performed the required card validity check using the CCL on each individual. The proposed rule also contains a regulatory provision indicating that TWIC reader records are SSI, and must be protected in accordance with 49 CFR part 1520.[81]

*O. Public Comment*

The Coast Guard invites comments on the risk-based approach to categorizing facilities and vessels and the assumptions and estimates used in the ''Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis,'' which is available in the public docket for this rulemaking. Specifically, the Coast Guard requests comments on the following:

1. We request comments from the public on the risk-based approach to classifying facilities and vessels including the use of MSRAM in the risk-based approach.

2. We request comments from the public regarding the incremental security benefits of requiring TWIC readers for higher-risk facilities and vessels. We request comments from the public on the security benefits of performing TWIC-holder identification, validation, and authentication via a TWIC reader instead of visual inspection.

3. We request comments from the public regarding the expected lifespan and replacement cycle for TWIC readers.

4. We request comments from owners and operators of Risk Group A facilities and vessels on the maintenance costs associated with the proposed TWIC reader requirements.

5. We request comments from owners and operator of MTSA-regulated vessels

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

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

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

and facilities already using TWIC readers, and whether the proposals in this NPRM would require additional investments, e.g., new readers or supporting infrastructure?

6. We request comments from owners and operators of MTSA-regulated vessels and facilities on the additional hours of TWIC reader training that would result from this proposed rule.

7. We request comments from the public regarding our estimates that it would take 25 hours to create an addendum for each VSP and FSP.

8. We request comments from the public on potential delays due to TWIC reader use and the associated cost estimates used in this proposed rule.

9. We request comments from owners and operator of MTSA-regulated vessels and facilities already using TWIC readers on the types and frequency of TWIC reader failures.

10. We request comments from the public on the expected rates at which TWICs will need to be replaced during implementation and all subsequent years.

11. We request comments from owners and operators of Risk Group A vessels and facilities regarding whether they intend to require the use of PINs, how often will PINs be used, and in what scenarios. What percentage of TWIC-holders do not currently remember their PIN, and also how many TWIC-holders are anticipated to travel to an enrollment center to retrieve their PIN?

12. We request comments from the public on the anticipated frequency of the use of an escort and the availability of escorts to provide access to secure areas in the cases of an invalid TWIC reader transaction.

13. We request comments from the public on any additional costs or benefits to TWIC reader requirements not accounted for in this NPRM.

14. We have clarified in the preamble to this NPRM that a facility that receives Risk Group A vessels would be categorized as a Risk Group A facility. We request additional comments from the public on specific scenarios that might warrant further consideration of potential regulatory requirements to address the interaction of vessels and facilities in different risk groups.

15. We seek comments from the public on whether the additional flexibility of being able to modify a facility's security footprint by assigning different portions of the facility to different risk groups is necessary or appropriate. Please be as specific as possible in explaining how this would apply to your facility.

16. We request comments from the public regarding practical scenarios in which a vessel might not be able to download necessary CCL updates within the prescribed frequency (weekly or daily, depending on MARSEC Level). Additionally, we request comments from the public regarding the regulatory requirements that we should put in place when vessels are in one of those scenarios. In those scenarios, should we require the use of TWIC readers for identity verification, card authentication, and card validity, even though the CCL might not have been updated within the prescribed frequency? Should we require the owner or operator to update the CCL at the next available opportunity? What other alternatives should we consider?

17. We request comments from the public on the proposed regulatory provisions regarding the placement of TWIC readers for vessels and facilities, and how to minimize crewmembers from entering secure and/or restricted areas if they do not hold a TWIC.

18. We request comments from the public regarding whether 7 days is a sufficient amount of time in which to expect resolution of a typical TWIC reader or communication systems malfunction.

19. We request comments from the public on the proposal to exempt all vessels with 14 or fewer TWIC-holding crewmembers from TWIC reader requirements, including whether 14 is an appropriate cut-off number. Please explain and provide available data to support your comments.

20. We request comments from the public on whether any or all of petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities should be categorized in Risk Group A. We also request comments from the public on how to define these facilities for the purpose of this rulemaking.

21. We request comments from the public on whether there is a population of State-licensed vessel pilots that are not otherwise required to obtain a TWIC because they access secure areas of MTSA-regulated vessels.

22. We request comments from the public on the proposal for Risk Group A to update CCL information at different frequencies (weekly or daily) depending on MARSEC Level.

23. We request comments from the public on whether this rule may help to reduce criminal activity at ports and on vessels. Please describe any anecdotal evidence or data to support your comments.

24. We request comments from the public on the characterizations and conclusions in the preamble to this NPRM of the TWIC Pilot, and how we used the findings from the TWIC Pilot to inform the NPRM.

25. We request comments from the public on any other matters relevant to the proposals in this NPRM and whether there are additional data sources that we should consider. If there are, please include information in your comments about these data sources and the reason for their relevance.

## V. Regulatory Analyses

We developed this proposed rule after considering numerous statutes and executive orders related to rulemaking. Below we summarize our analyses based on 13 of these statutes or executive orders.

### *A. Regulatory Planning and Review*

Executive Orders 12866 (''Regulatory Planning and Review'') and 13563 (''Improving Regulation and Regulatory Review'') direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This proposed rule is a significant regulatory action under section 3(f) of Executive Order 12866, Regulatory Planning and Review. OMB has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. A draft Assessment is available in the docket where indicated under the ''Public Participation and Request for Comments'' section of this preamble. A summary of the Assessment follows:

We propose amending our regulations on certain MTSA-regulated vessels and facilities to include requirements for electronic TWIC readers to be used for access control for unescorted access to secure areas.

The following table summarizes the costs and benefits of this proposed rule.

TABLE 1—SUMMARY OF COSTS AND BENEFITS [82]

| Category | NPRM |
|---|---|
| Applicability | High-risk MTSA-regulated facilities and high risk MTSA-regulated vessels with greater than 14 TWIC-holding crew. |
| Affected Population | 38 vessels.<br>532 facilities. |
| Costs ($ millions, 7% discount rate) | $26.5 (annualized).<br>$186.1 (10-year). |
| Costs (Qualitative) | Time to retrieve or replace lost PINs for use with TWICs. |
| Benefits (Qualitative) | Standardization of access control and credential verification throughout industry.<br>Enhanced access control and security at U.S. maritime facilities and onboard U.S. flagged vessels.<br>Reduction of human error when checking identification and manning access points. |

In this NPRM, we propose to require owners and operators of certain vessels and facilities regulated by the Coast Guard under 33 CFR Chapter I, subchapter H, to use electronic readers designed to work with TWIC as an access control measure. This NPRM also proposes additional requirements associated with electronic TWIC readers, including recordkeeping requirements for those owners and operators required to use an electronic TWIC reader, and amendments to security plans previously approved by the Coast Guard to incorporate TWIC requirements.

The proposals in this NPRM, once final, would enhance the security of vessels, ports, and other facilities by ensuring that only individuals who hold TWICs are granted unescorted access to secure areas at those locations. It would also further implement the MTSA transportation security card requirement, as well as the SAFE Port Act electronic TWIC reader requirements.

We estimate that this proposed rule would specifically affect owners and operators of MTSA-regulated vessels and facilities in Risk Group A with additional costs. As previously discussed, Risk Group A would consist of those vessels and facilities with highest consequence for a TSI. Affected facilities in Risk Group A would include: (1) Facilities that handle CDC in bulk; (2) Facilities that receive vessels certificated to carry more than 1,000 passengers; and (3) Barge fleeting facilities that receive barges carrying CDC in bulk. Affected vessels in Risk Group A would include: (1) Vessels that carry CDC in bulk; (2) Vessels certificated to carry more than 1,000 passengers; and (3) Towing vessels engaged in towing barges subject to (1) or (2). In addition, this proposal provides a TWIC Reader exemption for vessels with 14 or fewer TWIC-holding crewmembers, further reducing the number of affected vessels in Risk Group A.

Based on the risk-based hierarchy described in the preamble of this NPRM and data from the Coast Guard's MISLE database, we estimate this proposed rule would affect 532 facilities and 38 vessels with additional costs. All of these facilities and vessels are in Risk Group A.

To estimate the costs for this proposal, we use data from the TWIC Pilot, which was broken down by facility type, to estimate a cost per TWIC reader deployed for installation, integration, and PACS integration, where applicable. By distilling the costs from the TWIC Pilot down to a per TWIC reader cost by facility type, we are able to smooth out the varied costs in the TWIC Pilot and effectively normalize the TWIC Pilot costs before extrapolating out over the full affected population of this rulemaking.

The primary cost driver for this proposed rule is the capital cost associated with the purchase and installation of TWIC readers into access control systems. These costs include the cost of TWIC reader hardware and software, as well as costs associated with the installation, infrastructure, and integration with a PACS. Operational costs associated with this rulemaking, include security plan amendments, recordkeeping, CCL updates, training, and system maintenance. We also include operational and maintenance costs, which we estimate to be five percent of the cost of the TWIC reader hardware and software and are incurred annually. Table 2 shows the 10-year period of analysis for the total costs by facility type. These facility costs do not include costs associated with delays or replacement of TWICs, which are discussed later. These estimates include capital replacement costs for TWIC reader hardware and software beginning 5 years after implementation.

TABLE 2—10-YEAR TOTAL COSTS, BY FACILITY TYPE *

[$ Millions]

| Year | Bulk liquid | Break bulk and solids | Container | Large passenger | Small passenger | Mixed use | Total |
|---|---|---|---|---|---|---|---|
| 1 | $37.2 | $2.7 | $0.9 | $11.3 | $5.0 | $5.0 | $62.2 |
| 2 | 38.1 | 2.8 | 0.9 | 11.6 | 5.2 | 5.2 | 63.8 |
| 3 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |
| 4 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |
| 5 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |
| 6 | 14.1 | 1.0 | 0.3 | 4.3 | 1.9 | 1.9 | 23.6 |
| 7 | 14.1 | 1.0 | 0.3 | 4.3 | 1.9 | 1.9 | 23.6 |
| 8 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |
| 9 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |

[82] For a more detailed discussion of costs and benefits, see the full Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis available on the docket for this rulemaking. Appendix G of that document outlines the costs by provision and also discusses the complementary nature of the provisions and the subsequent difficulty in distinguishing independent benefits from individual provisions.

TABLE 2—10-YEAR TOTAL COSTS, BY FACILITY TYPE *—Continued

[$ Millions]

| Year | Bulk liquid | Break bulk and solids | Container | Large passenger | Small passenger | Mixed use | Total |
|---|---|---|---|---|---|---|---|
| 10 | 2.0 | 0.1 | 0.0 | 0.6 | 0.3 | 0.3 | 3.3 |
| Total Undiscounted | 115.3 | 8.4 | 2.7 | 35.2 | 15.7 | 15.6 | 193.0 |
| *Total Discounted at 7%* | *94.0* | *6.9* | *2.2* | *28.7* | *12.8* | *12.7* | *157.2* |
| *Total Discounted at 3%* | *105.1* | *7.7* | *2.5* | *32.1* | *14.3* | *14.2* | *175.9* |

Note: Numbers may not total due to rounding.

*These facilities are regulated because they handle CDC or more than 1,000 passengers. In the U.S. marine transportation system, facilities often handle a variety of commodities and provide a variety of commercial services. These facility types have different costs based on physical characteristics, such as the number of access points that would require TWIC readers, and other data received from the TWIC Pilot Study. See the Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis for details on different facility types and data from the TWIC Pilot Study.

To account for potential opportunity costs associated with the delays as a result of the TWIC reader requirements, we estimate a cost of delay associated with failed reads.[83] We provide a range of delay costs based on different delays in seconds and also based on the number of times a TWIC-holder may have their card read on a weekly basis. By using a range of delay costs, we are able to account for multiple scenarios where an invalid TWIC reader transaction would lead to the use of a secondary processing operation, such as a visual inspection, additional identification validation, or other provisions as set forth in the FSP.[84]

TABLE 3—COST OF DELAYS DUE TO INVALID TRANSACTION PER YEAR, FOR RISK GROUP A FACILITIES

| | 1 Read per week | 2 Reads per week | 3 Reads per week | 4 Reads per week | 5 Reads per week | Average |
|---|---|---|---|---|---|---|
| 6 Seconds | $91,244 | $182,489 | $273,733 | $364,977 | $456,221 | $273,733 |
| 14 Seconds | 212,903 | 425,807 | 638,710 | 851,613 | 1,064,517 | 638,710 |
| 30 Seconds | 456,221 | 912,443 | 1,368,664 | 1,824,886 | 2,281,107 | 1,368,664 |
| 60 Seconds | 912,443 | 1,824,886 | 2,737,328 | 3,649,771 | 4,562,214 | 2,737,328 |
| 120 Seconds | 1,824,886 | 3,649,771 | 5,474,657 | 7,299,543 | 9,124,428 | 5,474,657 |
| Average | 699,539 | 1,399,079 | 2,098,618 | 2,798,158 | 3,497,697 | 2,098,618 |

For the purposes of this analysis, we used the cost of delay estimate of $2.1 million per year, which represents the average delay across all iterations of delay times and TWIC reader transactions.

The use of TWIC readers would also increase the likelihood of faulty TWICs (TWICs that are not machine readable) being identified and the need for secondary screening procedures so affected workers and operators can address these issues.[85] If a TWIC-holder's card is faulty and cannot be read, the TWIC-holder would need to travel to a TWIC Enrollment Center to get a replacement TWIC, which results in additional travel and replacement costs. To account for this, we estimate a cost for a percentage of TWIC-holders to obtain replacement TWICs.

Based on information from the TWIC Pilot, we estimate that approximately five percent of TWIC-holders associated with Risk Group A would need to replace TWICs that cannot be read. We estimate that this would cost approximately $262.37 per TWIC-holder to travel to a TWIC Enrollment center and get a replacement TWIC.[86] Overall, we estimate that TWIC replacement would cost approximately $1.9 million per year for TWIC transactions involving Risk Group A facilities. We assume this is an annual cost, though we anticipate that the rate of TWIC replacements will decrease as TWIC reader use increases, since the number of unreadable TWICs initially identified will decrease as the regular use of TWIC readers will serve to enhance TWIC validity and readability.

Table 4 shows the average initial phase-in and annual recurring costs per facility by facility type. This includes capital, operational, delay, and TWIC replacement costs due to invalid TWIC reader transactions. It does not, however, account for vessel costs. Table 5 shows the total cost to facilities over the 10-year period of analysis by facility type. This includes capital, operational, delay, and TWIC replacement costs due to invalid TWIC reader transactions.

[83] Delays may result from operational, human- or weather-related factors.

[84] The Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis contains a discussion of the different failure mode scenarios where an invalid TWIC reader transaction would lead to potential delays and the use of secondary processing.

[85] Although current regulations require that TWICs be valid and readable upon request by DHS or law enforcement personnel, we anticipate that widespread use of TWIC readers will initially identify more unreadable cards. However, we expect the regular use of TWIC readers to ultimately serve to enhance compliance with current TWIC card validity and readability requirements.

[86] This cost is explained in greater detail in the Preliminary Regulatory Analysis and Initial Regulatory Flexibility Analysis. It includes an estimated $202.37 for the average TWIC-holder to travel to a TWIC Enrollment Center, cost to be away from work, wait time at the Enrollment Center, and the $60 fee for a replacement TWIC. Some TWIC-holders may not need to pay a replacement fee if the TWIC is determined faulty as a result of the card production process. However, these TWIC-holders would still need to travel to a TWIC Enrollment Center to get a replacement TWIC.

TABLE 4—PER FACILITY COST, BY FACILITY TYPE

| Phase-in & recurring costs | Bulk liquid | Break bulk and solids | Container | Large passenger | Small passenger | Mixed use |
|---|---|---|---|---|---|---|
| Initial Phase-in Cost | $256,267 | $347,901 | $604,007 | $252,324 | $164,011 | $169,136 |
| Annual Recurring cost | 14,531 | 19,727 | 34,248 | 14,307 | 9,300 | 9,590 |
| Annual Recurring cost *with* Equipment Replacement | 94,399 | 128,154 | 222,493 | 92,947 | 60,415 | 62,303 |

TABLE 5—10-YEAR TOTAL COST RISK GROUP A FACILITIES, BY FACILITY TYPE *

[$ Millions]

| Year | Bulk liquid | Break bulk and solids | Container | Large passenger | Small passenger | Mixed use | Total |
|---|---|---|---|---|---|---|---|
| 1 | $38.3 | $2.8 | $0.9 | $11.7 | $5.2 | $5.2 | $64.2 |
| 2 | 40.5 | 3.0 | 1.0 | 12.4 | 5.5 | 5.5 | 67.8 |
| 3 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| 4 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| 5 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| 6 | 16.5 | 1.2 | 0.4 | 5.0 | 2.2 | 2.2 | 27.6 |
| 7 | 16.5 | 1.2 | 0.4 | 5.0 | 2.2 | 2.2 | 27.6 |
| 8 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| 9 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| 10 | 4.3 | 0.3 | 0.1 | 1.3 | 0.6 | 0.6 | 7.3 |
| Total Undiscounted | 137.9 | 10.1 | 3.3 | 42.1 | 18.7 | 18.7 | 230.8 |
| *Total Discounted at 7%* | *$109.6* | *$8.0* | *$2.6* | *$33.4* | *$14.9* | *$14.9* | *$183.3* |
| *Total Discounted at 3%* | *$124.2* | *$9.1* | *$3.0* | *$37.9* | *$16.9* | *$16.8* | *$207.9* |

* This table includes the costs to facilities as well as additional costs such as delay, travel, and TWIC replacement costs due to TWIC failures.

For the 38 Risk Group A vessels with greater than 14 TWIC-holding crewmembers, we assume that each vessel will comply with the requirements by purchasing two portable TWIC readers and deploying them at the main access points of the vessel. We estimate the annualized costs to vessels of this rulemaking to be approximately $0.4 million at a 7 percent discount rate. These costs are shown in Table 6.

TABLE 6—TOTAL VESSEL COSTS

[Risk Group A with more than 14 TWIC-holding crewmembers] *

| Year | Undiscounted | 7% | 3% |
|---|---|---|---|
| 1 | $1,257,866 | $1,175,576 | $1,221,229 |
| 2 | 132,114 | 115,394 | 124,530 |
| 3 | 132,114 | 107,845 | 120,903 |
| 4 | 132,114 | 100,789 | 117,382 |
| 5 | 132,114 | 94,196 | 113,963 |
| 6 | 1,145,036 | 762,986 | 958,949 |
| 7 | 132,114 | 82,274 | 107,421 |
| 8 | 132,114 | 76,892 | 104,292 |
| 9 | 132,114 | 71,861 | 101,255 |
| 10 | 132,114 | 67,160 | 98,305 |
| Total | $3,459,815 | $2,654,972 | $3,068,229 |
| Annualized | ..... | 378,008 | 359,690 |

* Because the affected population is relatively small, we assume that all 38 vessels will comply within the first year of implementation. However, owners and operators of these vessels would have 2 years to comply with the rulemaking.

We estimate the annualized cost of this proposed rule to industry over 10 years to be about $26.5 million at a 7 percent discount rate. The main cost drivers of this proposed rule are the acquisition and installation of TWIC readers and the maintenance of the affected entity's TWIC reader system. Initial costs, which would be distributed over a 2-year implementation phase, consist predominantly of the costs to purchase and install TWIC readers and to integrate them with owners' and operators' PACS. Annual costs would be driven by costs associated with CCL updates, recordkeeping, training, system maintenance and opportunity costs associated with failed reader transactions.

We estimated the present value average costs of this proposed rule on industry for a 10-year period as summarized in Table 7. The costs were discounted at 3 and 7 percent as set forth by guidance in OMB Circular A–4.

TABLE 7—TOTAL INDUSTRY COST, RISK GROUP A

[$ Millions]

| Year | Facility | Vessel | Additional costs* | Undiscounted | 7% | 3% |
|---|---|---|---|---|---|---|
| 1 | $62.2 | $1.3 | $2.0 | $65.4 | $61.1 | $63.5 |
| 2 | 63.8 | 0.1 | 4.0 | 67.9 | 59.3 | 64.0 |
| 3 | 3.3 | 0.1 | 4.0 | 7.4 | 6.0 | 6.8 |
| 4 | 3.3 | 0.1 | 4.0 | 7.4 | 5.6 | 6.6 |
| 5 | 3.3 | 0.1 | 4.0 | 7.4 | 5.3 | 6.4 |
| 6 | 23.6 | 1.1 | 4.0 | 28.7 | 19.2 | 24.1 |
| 7 | 23.6 | 0.1 | 4.0 | 27.7 | 17.3 | 22.6 |
| 8 | 3.3 | 0.1 | 4.0 | 7.4 | 4.3 | 5.8 |
| 9 | 3.3 | 0.1 | 4.0 | 7.4 | 4.0 | 5.7 |
| 10 | 3.3 | 0.1 | 4.0 | 7.4 | 3.8 | 5.5 |
| Total | 193.0 | 3.5 | 37.8 | 234.2 | 186.0 | 210.9 |
| Annualized | | | | | 26.5 | 24.7 |

*This includes additional delay, travel, and TWIC replacement costs due to TWIC failures.

As this rule would require amendments to FSPs and VSPs, we estimate a cost to the government to review these amendments during the implementation period. We do not anticipate any additional annual cost to the government from this rulemaking. For the total implementation period, the total government cost would be $98,226 at a 7 percent discount rate. Table 8 shows the 10-year government costs.

TABLE 8—GOVERNMENT COSTS*

| | FSP | VSP | Total undiscounted | 7% | 3% |
|---|---|---|---|---|---|
| 1 | $51,072 | $6,299 | $57,371 | $53,617 | $56,507 |
| 2 | 51,072 | 0 | 51,072 | 44,608 | 50,208 |
| 3 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 |
| Total | 102,144 | 6,299 | 108,443 | 98,226 | 103,840 |
| Annualized | | | | 13,985 | 12,173 |

*After implementation, we estimate there would be no additional government costs for plan review as additional updates would be covered under existing plan review requirements and resources.

Based on the proposals in this NPRM and recent data, we estimated the average first-year cost of this NPRM (combined industry and government) to be about $61.2 million or $63.6 million at a 7 or 3 percent discount rate, respectively. The undiscounted annual recurring cost for this proposal is approximately $7.4 million in every year except years 6 and 7, due to equipment replacement 5 years after implementation. The annualized cost of this proposed rule is $26.5 million at 7 percent and $24.7 million at 3 percent. The 10-year cost to industry of this proposed rule is approximately $186.1 million at a 7 percent discount rate, and $211.0 million at a 3 percent discount rate, respectively.

The benefits of the proposed rule include enhancing the security of vessels, ports, and other facilities by ensuring that only individuals who hold TWICs are granted unescorted access to secure areas at those locations.

TWIC readers will make identification, validation, and verification of individuals attempting to gain unescorted access to a secure area more reliable and also will help to alleviate potential sources of human error when checking credentials at access points. Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. Card authentication ensures that the TWIC is not counterfeit, and card validation ensures that the TWIC has not expired or been revoked by TSA, or reported as lost, stolen, or damaged. Furthermore, the standardization of TWIC readers on a national scale could provide additional benefits in the form of efficiency gains in implementing access control systems throughout port facilities and nationally for companies operating in multiple locations.

The proposed rule would also further implement the MTSA provision for the transportation security card requirement, as well as the SAFE Port Act electronic TWIC reader requirements. Due to current data limitations, we do not estimate monetized benefits of this proposed rule. We present qualitative benefits and a break-even analysis in this preliminary analysis.

Break-even analysis is useful when it is not possible to quantify the benefits

of a regulatory action.[87] OMB Circular A–4 recommends a ''threshold'' or ''break-even'' analysis when non-quantified benefits are important to evaluating the benefits of a regulation. Threshold or break-even analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?'' [88] For this rulemaking, we calculate a potential range of break-even results from the estimated consequences of the three attack scenarios that are most likely to be mitigated by the use of TWIC readers. Because the primary function of the TWIC card and TWIC reader is to enhance access control and identity verification and validation, the attack scenarios evaluated within MSRAM to provide the consequence data for this analysis were limited to the following:

- Truck Bomb
  - Armed terrorists use a truck loaded with explosives to attack the target focal point. The terrorists will attempt to overcome guards and barriers if they encounter them.
- Terrorist Assault Team
  - A team of terrorists using weapons and explosives attack the target focal point. Assume the terrorists have done prior planning and surveillance, but have no insider support of assault.
- Passenger/Passerby Explosives/ Improvised Explosive Device
  - Terrorists exploit inadequate access control and detonate carried explosives at the target focal point. Assume the terrorists approach the target under cover of legitimate presence and are not armed. Note: for this attack mode, terrorist is not an insider.

The focus on these three attack scenarios allows us to look at specific attack scenarios that are most likely to be mitigated by the use of TWIC readers. We base our analysis on the highest consequence scenario of these three for each target. These scenarios were chosen because they represent the scenarios most likely to benefit from the enhanced access control afforded by TWIC readers, as they require would-be attackers gaining access to the target in question. For these three attack types, the aggressor would first need to gain access to the facility to inflict maximum damage. Because the function of the TWIC reader is to enhance access control, the deployment of TWIC readers would increase the likelihood of identifying and denying access to an individual attempting nefarious acts. The consequence of an attack scenario is dependent on both the target and the attack mode. The attack modes selected for this analysis, as described above, serve to limit the potential maximum consequence compared to other potential attack modes. Typically, one or more threat, vulnerability, or consequence drivers will contribute significantly more to a target's risk scores than others; these are known as major risk drivers. The local COTPs document major risk drivers such as inherent limitations on access control or the potential death and injury during the analysis process.

For the break-even analysis, we estimate the consequences of these three scenarios by estimating the number of casualties and serious injuries that would occur had the attack been successful. To monetize the value of fatalities prevented, we use the concept of ''value of a statistical life'' (VSL), which is commonly used in safety and security analyses. The VSL does not represent the dollar value of a person's life, but the amount society would be willing to pay to reduce the probability of death. We currently use a value of $6.3 million as an estimate of VSL.[89] This break-even analysis does not consider any property damage, environmental damage, indirect or macroeconomic consequences these terrorist attacks might cause. Consequently, the economic impacts of the terrorist attacks estimated for this series of break-even analyses would be higher if these other impacts were considered. See Table 9 for the average maximum consequence [90] of the three attack scenarios on Group A facilities.

TABLE 9—ANNUAL RISK REDUCTION AND ATTACKS AVERTED REQUIRED FOR COSTS TO EQUAL BENEFITS, NPRM ALTERNATIVE

| | Annualized cost, 7% discount rate ($ millions) | Average consequence ($ millions) | Required reduction in risk | Frequency of attacks averted |
|---|---|---|---|---|
| NPRM Alternative | $26.5 | $3,468.7 | 0.8% | One every 130.9 years. |

As shown in Table 9, an avoided terrorist attack at an average target is equivalent to $3,468.7 million in avoided consequences. Using the estimated annualized cost of this regulation, the annual reduction in the probability of attack to a Risk Group A facility that would just equate avoided consequences with cost is less than 1 percent. To state this in another way, if implementing this regulation would lower the likelihood of a successful terrorist attack by more than 1 percent each year, then this would be a socially efficient use of resources. This proposed rule is estimated to cost approximately $26.5 million annually. This proposed rule would be cost effective if it prevented one terrorist attack with consequence equal to the average every 130.9 years ($3,468.7/$26.5). These small changes in risk reduction suggest the potential benefits of the proposed rule justify the costs.

For the NPRM alternative, we assess that all Risk Group A facilities will be required to install and use TWIC readers. On the vessel side, we assess that all Risk Group A vessels with a crew size greater than 14 TWIC-holding crewmembers will likely carry two portable TWIC readers. For this alternatives analysis, we look at several different ways to implement TWIC reader requirements based on the risk group hierarchy. These alternatives include requiring TWIC readers for Risk Group A and B facilities, along with Risk Group A vessels with more than 14 TWIC-holding crewmembers, Risk

[87] In order to monetize the benefits from an anti-terrorism regulation, we would need to know the incremental reduction in risk of a successful terrorist attack that would accrue from the regulatory action being analyzed. However, the data needed to estimate this reduction in risk are not available.

[88] U.S. Office of Management and Budget, Circular A–4, September 17, 2003.

[89] ''Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses,'' prepared for the U.S. Customs and Border Protection, June 2008. See *www.regulations.gov,* search on docket USCG–2005–21869–003.

[90] The average maximum consequence is the average of the highest consequence attack scenario for each target in the referenced target group. The average maximum consequence compares the results from the three analyzed attack modes for each target and averages the maximum consequence for all targets.

Group A and container facilities, along with Risk Group A vessels with more than 14 TWIC-holding crewmembers, adding certain high-risk facilities to Risk Group A, including petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities, and Risk Group A facilities and all self-propelled Risk Group A vessels. Table 10 summarizes the alternatives considered. The costs displayed are the 10-year costs and the 10-year annualized cost, each discounted at 7 percent.

TABLE 10—REGULATORY ALTERNATIVES

| | Description | Facility population | Vessel population | Total cost ($ millions, at 7% discount rate) | Annualized cost ($ millions, at 7% discount rate) |
|---|---|---|---|---|---|
| NPRM Alternative | All Risk Group A facilities and Risk Group A vessels with more than 14 crewmembers. | 532 | 38 | $186.1 | $26.5 |
| Alternative 2 | All Risk Group A facilities and Risk Group A vessels (except barges). | 532 | 138 | 197.7 | 28.2 |
| Alternative 3 | Risk Group A and all container facilities and Risk Group A vessels with more than 14 crewmembers. | 651 | 38 | 624.9 | 89.0 |
| Alternative 4 | All Risk Group A facilities, plus additional high consequence facilities including petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities, and Risk Group A vessels with more than 14 crewmembers. | 1,174 | 38 | 419.6 | 59.7 |
| Alternative 5 | Risk Group A and B Facilities and Risk Group A vessels with more than 14 crewmembers. | 2,173 | 38 | 991.6 | 141.2 |

When comparing alternatives, we also looked at the results of the break-even analysis for these alternatives. As Table 11 shows, for the overall average maximum consequence, the NPRM alternative would require the lowest reduction in risk for the costs of the rule to be justified. As the purpose of this rulemaking is to enhance security to mitigate a TSI, we assess the break-even for the overall consequence of a TSI. It is assumed that the highest consequence targets will be the most attractive targets for potential terrorist attack.

TABLE 11—SUMMARY OF REQUIRED RISK REDUCTION AND ATTACKS AVERTED BY REGULATORY ALTERNATIVE, OVERALL

[In $ millions]

| | Annualized cost, 7% discount rate | Average consequence | Required reduction in risk (percent) | Frequency of attacks averted |
|---|---|---|---|---|
| NPRM Alternative | $26.5 | $3,468.7 | 0.8 | One every 130.9 years. |
| Risk Group A facilities and all Risk Group A vessels, except barges. | 28.2 | 3,468.7 | 0.8 | One every 123.2 years. |
| Risk Group A and all container facilities and Risk Group A vessels with more than 14 crewmembers. | 89.0 | 2,878.9 | 3.1 | One every 32.4 years. |
| All Risk Group A facilities, plus additional high consequence facilities including petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities, and Risk Group A vessels with more than 14 crewmembers. | 59.7 | 1,776.9 | 3.4 | One every 29.8 years. |
| Risk Groups A and B facilities and Risk Group A vessels with more than 14 crewmembers. | 141.2 | 1,143.3 | 12.4 | One every 8.1 years. |

NPRM Alternative—Risk Group A Facilities and Risk Group A Vessels With More Than 14 TWIC-Holding Crewmembers

The analysis for this alternative is discussed in detail previously in this section, as it is the alternative we propose in this NPRM.

Alternative 2—Risk Group A Facilities and All Risk Group A Vessels, Except Barges

This alternative would require TWIC readers to be used at all Risk Group A facilities and for all Risk Group A vessels, except barges. This alternative would increase the burden on industry and small entities by increasing the affected population from 38 vessels to 138 vessels. The number of facilities would be the same as in the NPRM alternative. Under this alternative, annualized cost of this rulemaking would increase from $26.5 million to $28.2 million, at a 7 percent discount rate. The discounted 10-year costs would go from $186.1 million to $197.7 million. While this alternative does not lead to a significant increase in costs, we reject it because requiring TWIC readers on vessels with 14 or fewer TWIC-holding crewmembers is unnecessary, as crews with that few members are known to all on the vessel. This crewmember limit was proposed in the ANPRM and was based on a recommendation from TSAC. In an effort to reduce unnecessary burden and minimize costs of this rulemaking, we estimate this is the most efficient way to regulate Risk Group A vessels. See the discussion in the NPRM on ''Recurring

Unescorted Access'' and ''TWIC Reader Requirements on Vessels'' for more details.

Alternative 3—Risk Group A and All Container Facilities and Risk Group A Vessels With More Than 14 TWIC-Holding Crewmembers

For this alternative, we assumed that only those facilities in Risk Group A, as previously defined, and all container facilities will require TWIC readers. This alternative would increase the burden on industry and small entities by increasing the affected population from 532 facilities to 651 facilities. Under this scenario, the annualized cost of this rulemaking would increase from $26.5 million to $89.0 million, at a 7 percent discount rate. The discounted 10-year costs would go from $186.1 million to $624.9 million. The inclusion of container facilities would also potentially have adverse environmental impacts due to increased air emissions due to longer wait (''cueing'') times and congestion at facilities.

We considered this alternative because container facilities are perceived to pose a unique threat to the maritime sector due to the transfer risk associated with containers. As discussed in the preamble of this NPRM, many of the high-risk threat scenarios at container facilities would not be mitigated by TWIC readers. The costs for TWIC readers at container facilities would not be justified by the amount of potential risk reduction at these facilities. While container facilities pose an increased transfer risk (i.e., there is a greater risk of a threat coming through a container facility and inflicting harm or damage elsewhere than with any other facility type), such threats are not mitigated by the use of TWIC readers. Furthermore, the use of TWIC readers, or other access control features, would not mitigate the threat associated with the contents of a container. The TWIC reader serves as an additional access control measure, but would not improve screening of cargoes for dangerous substances or devices. We request data and informed input regarding this assessment.

Alternative 4—Adding Certain High Consequence Facilities to Risk Group A (These Additional Facilities To Include Petroleum Refineries, Non-CDC Bulk Hazardous Materials Facilities, and Petroleum Storage Facilities)

For this alternative, we moved three facility categories—petroleum refineries, non-CDC bulk hazardous materials facilities, and petroleum storage facilities—into Risk Group A from Risk Group B based on the average maximum consequence for these facility types. This alternative would increase the burden on industry by increasing the affected population from 532 facilities to 1,174 facilities. Under this scenario, the annualized cost of this rulemaking would increase from $26.5 million to $59.7 million, at a 7 percent discount rate. The discounted 10-year costs would go from $186.1 million to $419.6 million.

We considered this alternative based on the high MSRAM consequence scores associated with these three facility types, as well as due to the perception that petroleum facilities pose a greater security risk than other facility types. Despite the high MSRAM consequence scores for these facility types, the overall risk scores as determined in the analytical hierarchy process (AHP) were not as high as those in the current Risk Group A, and therefore, we rejected this alternative and maintained the AHP-based risk groupings.

Alternative 5—Risk Group A and Risk Group B Facilities and Risk Group A Vessels With More Than 14 Crewmembers

Alternative 5 would require TWIC readers to be used at all Risk Group A and Risk Group B facilities, and Risk Group A vessels with greater than 14 TWIC-holding crewmembers. This alternative would increase the burden on industry and small entities by increasing the affected population from 532 facilities to 2,173 facilities. This increase in facilities would extend the affected population to facilities that fall under the second risk tier. Under this alternative, annualized cost of this rulemaking would increase from $26.5 million to $141.2 million, at a 7 percent discount rate. The discounted 10-year costs would go from $186.1 million to $991.6 million. Based on a recent study by HSI, as discussed in the preamble to this NPRM, the difference in risk between facilities in Risk Groups A and B is clearly defined, indicating that the two risk groups do not require the same level of TWIC requirements. Further, as discussed in the benefits section of this analysis, the break-even point, or the amount of risk that would need to be reduced for costs to equal benefits, for this alternative is much higher than that of the NPRM alternative. Moreover, we understand many of the comments opposing TWIC reader requirements represented the interests of owners and operators of vessels or facilities assigned to Risk Group B. For these reasons, we rejected this alternative.

The provisions in this proposed rule are taken in order to meet requirements set forth in MTSA and the SAFE Port Act. The proposal, as presented, represents the lowest cost alternative, as discussed above. We have focused this rulemaking on the highest risk population so as to reduce the impacts of this rule as much as possible. Also, we have created a performance standard that allows the affected population to implement the requirements in a manner most conducive to their own business practices. By allowing for flexibilities, such as the use of fixed or portable readers, and removing vessels with 14 or fewer TWIC-holding crewmembers from the requirements, we have reduced potential burden on all entities, including small entities. Furthermore, we believe that providing any additional relief for small entities would conflict with the purpose of this rulemaking, as the objective is to enhance access control and reduce risk of a TSI. Providing relief of the proposed requirements based on entity size would contradict that stated purpose and leave small entities, which may possess as great a risk as entities that exceed the Small Business Administration (SBA) size standards, more vulnerable to a TSI.

*B. Small Entities*

Under the Regulatory Flexibility Act (5 U.S.C. 601–612), we have considered whether this proposed rule would have a significant economic impact on a substantial number of small entities. The term ''small entities'' comprises 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 fewer than 50,000. An Initial Regulatory Flexibility Analysis discussing the impacts of this proposed rule on small entities is available in the docket where indicated under the **ADDRESSES** Section.

For this proposed rule, we estimated mandatory TWIC reader requirement costs for approximately 38 vessels and 532 facilities based on the risk assessment hierarchy and current data from the Coast Guard's MISLE database. Of these 532 facilities that would be affected by the TWIC reader requirements, we found 311 unique owners. Among these 311 unique owners, there were 31 government-owned entities, 119 companies that exceeded SBA small business size standards, 88 companies considered small by SBA size standards, and 73 companies for which no information was available. For the purposes of this analysis, we consider all entities for which information was not available to

be small. There were no not-for-profit entities in our affected population. Of the 31 government jurisdictions that would be affected by this proposed rule, 24 exceed the 50,000 population threshold as defined by the Regulatory Flexibility Act to be considered small and seven have government revenue levels such that there would not be an impact greater that 1 percent of government revenue.[91]

We were able to find revenue information for 64 of the 88 businesses deemed small by SBA size standards.[92] We then determined the impacts of the proposed rule on these companies by comparing the cost of the proposed rule to the average per facility cost of this rulemaking. To determine the average per facility cost, we average the per facility cost for all facility types using the same cost per facility type breakdown as used to assess the costs of this proposal. We then found what percent impact on revenue the proposed rule would have based on implementation costs (including capital costs) and annual recurring costs (including CCL updates, recordkeeping, and training). We estimate these costs to be, on average $233,736 per facility during the implementation period and $6,186 per facility in annual recurring cost.[93] We base our impact analysis on average cost to regulated entities due to the flexibility afforded by this proposed rule to individual facilities to determine how best to implement TWIC reader requirements.[94] Table 12 shows the potential revenue impacts for small businesses impacted by this rulemaking.

TABLE 12—REVENUE IMPACTS ON AFFECTED SMALL BUSINESSES—FACILITIES

| Revenue impact range | Impacts from implementation costs | | Impacts from recurring annual costs | |
|---|---|---|---|---|
| | Number of entities | Percent of entities | Number of entities | Percent of entities |
| 0% < Impact ≤ 1% | 27 | 42 | 57 | 89 |
| 1% < Impact ≤ 3% | 10 | 16 | 6 | 9 |
| 3% < Impact ≤ 5% | 5 | 8 | 1 | 2 |
| 5% < Impact ≤ 10% | 8 | 13 | 0 | 0 |
| Above 10% | 14 | 22 | 0 | 0 |
| Total | 64 | 100 | 64 | 100 |

The greatest impact is expected to occur during the implementation phase when 58 percent of small businesses that we were able to find revenue data on will experience an impact of greater than 1 percent, and 22 percent of small businesses that we were able to find revenue data on will experience an impact greater than 10 percent. After implementation, the impacts decrease and 89 percent of affected small businesses will see an impact less than 1 percent. We expect the revenue impacts for years with equipment replacement to be between those for implementation and annual impacts. During those years with equipment replacement, we estimate that approximately 44 percent of businesses would see an impact greater than 1 percent, and 13 percent would see an impact greater than 10 percent.[95]

For vessels, we found that for the 38 vessels that would be affected by this proposed rule, there were 10 unique owners, all of which were businesses. We were able to find employee and revenue data for all but one of the companies. Out of the nine companies for which we were able to find data, only two qualified as small businesses by SBA size standards. We estimate these costs to be, on average $33,102 per vessel during the implementation period, and $3,477 per vessel in annual cost. We base our impact analysis on average cost per vessel due to the flexibility afforded to vessels and the subsequent assumption that all vessels will deploy, on average, two portable TWIC readers. Both of these businesses would experience impacts less than 1 percent of revenue for both previously mentioned impact analyses.

If you think that your business, organization, or governmental jurisdiction qualifies as a small entity and that this proposed rule would have a significant economic impact on it, please submit a comment to the Docket Management Facility at the address under **ADDRESSES**. In your comment, explain why you think it qualifies and how and to what degree this proposed rule would economically affect it.

*C. Assistance for Small Entities*

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 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 proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult Lieutenant Commander Loan T. O'Brien, Coast Guard, telephone 202–372–1133. We will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the Coast Guard.

*D. Collection of Information*

This proposed 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(c), ''collection of information'' comprises reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. The title and description of the information collection, 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

[91] ''Government revenues'' used for this analysis include tax revenues, and in some cases, operating revenues for government owned waterfront facilities.

[92] SBA small business standards are based on either company revenue or number of employees. Many companies in our sample have employee numbers determining them small, but we were unable to find annual revenue data to pair with the employee data.

[93] These are weighted averages, based on the per facility cost displayed in Table 4 and the number of facilities by type.

[94] We do not know how a specific facility with comply with this rulemaking in regards to type and number of readers installed, number of personnel requiring training at a given facility, etc.

[95] We estimate an average cost per facility in years with equipment replacement to be $48,110.

completing and reviewing the collection.

Under the provisions of the proposed rule, the affected facilities and vessels would be required to update their FSPs and VSPs, as well as create and maintain a system of recordkeeping within 2 years of promulgation of the final rule. This requirement would be added to an existing collection with OMB control number 1625–0077.

*Title:* Security Plans for Ports, Vessels, Facilities, Outer Continental Shelf Facilities and Other Security-Related Requirements

*OMB Control Number:* 1625–0077.

*Summary of the Collection of Information:* This information collection is associated with the maritime security requirements mandated by MTSA. Security assessments, security plans, and other security-related requirements are found in 33 CFR chapter I, subchapter H. The proposed rule would require certain vessels and facilities to use electronic readers designed to work with the TWIC as an access control measure. Affected owners and operators would also face requirements associated with electronic TWIC readers, including recordkeeping requirements for those owners and operators required to use an electronic TWIC reader, and security plan amendments to incorporate TWIC requirements.

*Need for Information:* The information is necessary to show evidence that affected vessels and facilities are complying with the TWIC reader requirements.

*Proposed Use of Information:* We would use this information to ensure that facilities and vessels are properly implementing and utilizing TWIC readers.

*Description of the Respondents:* The respondents are owners and operators of certain vessels and facilities regulated by the Coast Guard under 33 CFR Chapter I, subchapter H.

*Number of Respondents:* The adjusted number of respondents is 13,825 for vessels, 3,270 for facilities, and 56 for OCS facilities. Of these 3,270 facilities and 13,825 vessels, approximately 532 facilities that are considered ''high risk'' would be required to modify their existing FSPs and approximately 38 vessels would be required to modify their VSPs to account for the TWIC reader requirements. These same populations would be required to create and maintain recordkeeping systems as well.

*Frequency of Response:* The FSP and VSP would need to be amended within 2 years of promulgation to include TWIC reader-related procedures. Recordkeeping requirements would need to be met along a similar timeline.

*Burden of Response:* The estimated burden for facilities would be 17,290 hours in the first year, 18,886 hours in the second year and 3,192 hours in the third year and all subsequent years. The burden for vessels would be 2,470 burden hours in year one, and 288 burden hours for all subsequent years. This includes an estimated 25 burden hours to amend the FSP or VSP, along with an implementation period burden of 40 hours and an annual burden of 6 hours for designing and maintaining a system of records for each facility or vessel, to include recordkeeping related to the CCL.

Estimate of Total Annual Burden

*Facilities:* The estimated burden over the 2-year implementation period for facilities is 25 hours per FSP amendment. Since there are currently 532 facilities that will need to amend their FSPs, the total burden on facilities would be 13,300 hours (532 FSPs × 25 hours per amendment) during the 2-year implementation period, or 6,650 hours each of the first 2 years. Facilities would also face a recordkeeping burden of 21,280 hours during the 2-year implementation period (532 facilities × 40 hours per recordkeeping system), or 10,640 hours each year over the first 2 years. There would also be an annual recordkeeping burden of 3,192 hours (532 facilities × 6 hours per year), starting in the third year. In the second year, the 266 facilities that implemented in the first year would incur the 6 hours of annual recordkeeping, at a burden of 1,596 (266 facilities × 6 hours). The total burden for facilities is estimated at 17,290 (6,650 + 10,640) in Year 1, 18,886 in Year 2 (6,650 + 10,640 + 1,596), and 3,192 in Year 3.

*Vessels:* For the 38 vessels, the burden in the first year would be 950 hours (38 VSPs × 25 hour per amendment). Vessels would also face a recordkeeping burden of 1,520 hours during the 1-year implementation period (38 vessels × 40 hours per recordkeeping system). There would also be an annual recordkeeping burden of 228 hours (38 vessels × 6 hours per year). The total burden for vessels is estimated at 2,470 (950 + 1,520) in Year 1 and 228 hours in Years 2 and 3.

*Total:* The total additional burden due to the TWIC Reader rule is estimated at 19,760 (2,470 for vessels and 17,290 for facilities) in Year 1, 19,114 (228 for vessels and 18,886 for facilities) in Year 2, and 3,420 (228 for vessels and 3,192 for facilities) in Year 3. The current annual burden listed in this collection of information is 1,108,043. The new burden, as a result of this proposed rulemaking, in Year 1 is 1,127,803 (1,108,043 + 19,760). The new burden, as a result of this proposed rule, is 1,127,803 (1,108,043 + 19,760). The total change in monetized burden in Year 1 is approximately $1.3 million. The total burden in Year 2 is 1,127,157 (1,108,043 + 19,114) and in Year 3 is 1,111,463 (1,108,043 + 3,420). The average annual additional burden across the 3 years is 14,098 and the average total burden is 1,122,141 (14,098 + 1,108,043).

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), we have submitted a copy of this proposed rule to OMB for its review of the collection of information.

We ask for public comment on the proposed collection of information to help us determine how useful the information is—whether it can help us perform our functions better, whether it is readily available elsewhere, how accurate our estimate of the burden of collection is, how valid our methods for determining burden are, how we can improve the quality, usefulness, and clarity of the information, and how we can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under **ADDRESSES**, by the date under **DATES**.

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 proposed collection.

*E. Federalism*

A rule has implications for Federalism under Executive Order 13132, Federalism, if it has a substantial direct effect on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government. This proposed rule has been analyzed in accordance with the principles and criteria in Executive Order 13132, and as discussed earlier in the preamble, it has been determined that this proposed rule does have Federalism implications or a substantial direct effect on the States.

This proposed rule would update existing regulations by creating a risk-based analysis of MTSA-regulated vessels and facilities. Based on this analysis, each vessel or facility is

classified according to its risk level, which then determines whether the vessel or facility would be required to use TWIC readers. Additionally, this proposed rule would amend recordkeeping requirements and add requirements to amend security plans in order to ensure compliance.

It is well-settled that States may not regulate in categories reserved for regulation by the Coast Guard. It is also well-settled, now, 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 fields foreclosed from regulation by the States or local governments. (See the decision of the Supreme Court in the consolidated cases of *United States* v. *Locke* and *Intertanko* v. *Locke,* 529 U.S. 89, 120 S.Ct. 1135 (March 6, 2000).)

The Coast Guard believes the Federalism principles articulated in *Locke* apply to this proposed rule since it would require certain MTSA-regulated vessels to carry TWIC readers (i.e., required equipment), and to conform to recordkeeping and security plan requirements. Therefore, States and local governments are foreclosed from regulating within this field. This principle also applies to MTSA-regulated facilities, at least insofar as a State or local law or regulation applicable to these same facilities for the purpose of their protection, would conflict with a Federal regulation (i.e., it would either actually conflict or would frustrate an overriding Federal need for uniformity).

Although State and local governments are foreclosed from regulating within this specific field, the Coast Guard recognizes the key role that State and local governments may have in making regulatory determinations. Additionally, Sections 4 and 6 of Executive Order 13132 require that for any rules with preemptive effect, the Coast Guard shall provide elected officials of affected State and local governments and their representative national organizations the notice and opportunity for appropriate participation in any rulemaking proceedings, and to consult with such officials early in the rulemaking process. Therefore, we invite affected State and local governments and their representative national organizations to indicate their desire for participation and consultation in this rulemaking process by submitting comments to this notice. In accordance with Executive Order 13132, the Coast Guard will provide a Federalism impact statement to document: (1) The extent of the Coast Guard's consultation with State and local officials that submit comments in response to this proposed rule; (2) a summary of the nature of any concerns raised by State or local governments and the Coast Guard's position thereon; and (3) a statement of the extent to which the concerns of State and local officials have been met.

*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 (adjusted for inflation) or more in any one year. Though this proposed rule would not result in such an expenditure, we do discuss the effects of this proposed rule elsewhere in this preamble.

*G. Taking of Private Property*

This proposed rule would not cause a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights.

*H. Civil Justice Reform*

This proposed rule meets applicable standards in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden.

*I. Protection of Children*

We have analyzed this proposed rule under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks. Though this proposed rule is a ''significant regulatory action'' under Executive Order 12866, it would not create an environmental risk to health or a risk to safety that might disproportionately affect children.

*J. Indian Tribal Governments*

This proposed rule does not have tribal implications under Executive Order 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 proposed rule under Executive Order 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. Though it is a ''significant regulatory action'' under Executive Order 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, it does not require a Statement of Energy Effects under Executive Order 13211.

*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 OMB, 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.

This proposed rule does not use technical standards. Therefore, we did not consider the use of voluntary consensus standards.

The Federal government is developing the TWIC reader standards. Under NTTAA and OMB Circular A–119, NIST is tasked with the role of encouraging and coordinating Federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST is assisting TSA with the establishment of a conformity assessment framework in support of a QTL for identity and privilege credential products, to be managed by TSA. NIST is also assisting TSA with the establishment of a testing suite for qualifying products in conformity to specified standards and TSA specifications.

If you are aware of voluntary consensus standards that might apply to this rule, please send a comment to the

docket using one of the methods under **ADDRESSES**. In your comment, please explain why you disagree with our analysis and/or identify voluntary consensus standards we have not listed that might apply.

*M. Environment*

We have analyzed this proposed rule under DHS Management Directive 023–01 and Commandant Instruction M16475.lD, which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4370f), and have made a preliminary determination that this action is not likely to have a significant effect on the human environment. A ''Draft Programmatic Environmental Assessment'' (DPEA) and a draft ''Finding of No Significant Impact'' (FONSI) are available in the docket where indicated under the ''Public Participation and Request for Comments'' section of this preamble. Our analysis indicates that TWIC reader operations would have insignificant direct, indirect or cumulative impacts on environmental resources, with special attention to potential air quality issues. We encourage the public to submit comments on the DPEA and draft FONSI.

**List of Subjects**

*33 CFR Part 101*

Harbors, Incorporation by reference, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

*33 CFR Part 104*

Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels.

*33 CFR Part 105*

Maritime security, Reporting and recordkeeping requirements, Security measures.

*33 CFR Part 106*

Continental shelf, Maritime security, Reporting and recordkeeping requirements, Security measures.

For the reasons discussed in the preamble, we propose to amend 33 CFR parts 101, 104, 105, and 106 as follows:

## 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. Amend § 101.105, as follows:

■ a. Add, in alphabetical order, definitions for the terms ''Biometric match'', ''Canceled Card List (CCL)'', ''Card authentication'', ''Card Holder Unique Identifier (CHUID)'', ''Card validity check'', ''Mobile Offshore Drilling Unit (MODU)'', ''Offshore Supply Vessel (OSV)'', ''Physical Access Control System (PACS)'', ''Risk Group'', and ''TWIC reader''; and

■ b. Remove the definition for the term ''Recurring unescorted access''.

The additions read as follows:

### § 101.105 Definitions.

* * * * *

*Biometric match* means a confirmation that: one of the two biometric (fingerprint) templates stored in the Transportation Worker Identification Credential (TWIC) matches the scanned fingerprint of the person presenting the TWIC; or the alternate biometric stored in a PACS matches the corresponding biometric of the person.

* * * * *

*Canceled Card List (CCL)* means the list of TWIC Federal Agency Smart Credential-Numbers (FASC—Ns) that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or because the card has been reported lost, stolen, or damaged.

* * * * *

*Card authentication* means electronic verification that the TWIC is a valid credential issued by TSA, containing the Card Holder Unique Identifier (CHUID) and the correct digital signature.

*Card Holder Unique Identifier (CHUID)* means the standardized data object comprised of the FASC—N, globally unique identifier, expiration date, and certificate used to validate the data integrity of other data objects on the credential.

*Card validity check* means electronic verification that the TWIC has not been invalidated or revoked by checking the TWIC against the Canceled Card List or, for vessels and facilities assigned to Risk Group B or C according to §§ 104.263 or 105.253 of this subchapter, by verifying that the expiration date on the face of the TWIC has not passed.

* * * * *

*Mobile Offshore Drilling Unit (MODU)* means the same as defined in 33 CFR 140.10.

* * * * *

*Offshore Supply Vessel (OSV)* means the same as defined in 46 CFR 125.160.

* * * * *

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

* * * * *

*Risk Group* means the risk ranking assigned to a vessel, facility, or OCS facility according to §§ 104.263, 105.253, or 106.258 of this subchapter, for the purpose of the TWIC requirements in this subchapter.

* * * * *

*TWIC reader* means an electronic device listed on TSA's Qualified Technology List (QTL) and used to verify and validate: the authenticity of a TWIC; the identity of the TWIC-holder as the legitimate bearer of the credential; that the TWIC is not expired; and that the TWIC is not on the CCL. TSA's QTL of acceptable TWIC readers may be accessed online at http://(TBD).

* * * * *

■ 3. Add § 101.112 to read as follows:

### § 101.112 Federalism.

(a) The regulations in 33 CFR parts 101, 103, 104, and 106 have preemptive effect over State or local regulation within the same field.

(b) The regulations in 33 CFR part 105 have preemptive effect over State or local regulations insofar as a State or local law or regulation applicable to the facilities covered by part 105 would conflict with the regulations in part 105, either by actually conflicting or frustrating an overriding Federal need for uniformity.

### § 101.514 [Amended]

■ 4. In § 101.514, remove paragraph (e).

■ 5. Revise § 101.515(d)(2) to read as follows:

### § 101.515 TWIC/Personal identification.

* * * * *

(d) * * *

(2) Each person who has been issued or who possesses a TWIC must allow their TWIC to be read by a TWIC reader and must submit their reference biometric, such as a fingerprint, and any other required information, such as a Personal Identification Number (PIN), to the TWIC reader, upon a request from TSA, the Coast Guard, any other authorized DHS representative, or a Federal, State, or local law enforcement officer.

■ 6. Add § 101.520 to read as follows:

### § 101.520 TWIC reader requirements for Risk Group A.

Owners or operators of vessels or facilities subject to part 104 or 105 of this subchapter that are assigned to Risk Group A in §§ 104.263 or 105.253 of this

subchapter must ensure that a Transportation Worker Identification Credential (TWIC) program is implemented as follows:

(a) *Maritime Security (MARSEC) Level 1.* (1) Prior to each entry, all persons must present their TWICs for inspection using a TWIC reader, with or without a Physical Access Control System (PACS), before being granted unescorted access to secure areas. The TWIC inspection must include an identity verification including a biometric match, card authentication, and card validity check using Canceled Card List (CCL) information that is no more than 7 days old.

(2) With a PACS, biometrics other than the fingerprint templates stored in the TWIC may be used to perform the identity verification, provided that the owner or operator links the person, the TWIC, and the alternate biometric in the PACS. To do this, a one-time initial biometric match and card authentication using a TWIC reader must be performed. Owners and operators must update their security plans to explain how the PACS performs the required security functions and how they protect sensitive security information.

(b) *MARSEC Levels 2 and 3.* At these MARSEC Levels, the same procedures outlined in paragraph (a) of this section must be used, except that the card validity check must use CCL information that is no more than 1 day old.

(c) The CCL information used to verify card validity must be updated within 12 hours of any increase in MARSEC Level, no matter when the information was last updated.

(d) Only the most recently obtained CCL information shall be used to conduct card validity checks.

(e) Vessels in Risk Group A with more than 14 crewmembers required to hold a TWIC must comply with the applicable TWIC reader requirements in this subchapter. All vessels with 14 or fewer TWIC-holding crewmembers are exempt from the TWIC reader requirements in this subchapter. Owners or operators of vessels with 14 or fewer TWIC-holding crewmembers are required to perform the following TWIC visual inspection requirements, prior to each entry, on persons seeking unescorted access to secure areas:

(1) Visually match the photograph on the TWIC to the person presenting the TWIC.

(2) Visually check the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(3) Visually verify that the expiration date on the face of the TWIC has not passed.

(f) If the COTP determines that TWIC reader requirements are causing delays at a facility that result in excessive vehicle build-up or other consequence, the COTP is authorized to temporarily suspend TWIC reader requirements at that facility, and permit the owner or operator to satisfy the requirements of this section by performing the following TWIC visual inspections, prior to each entry, on persons seeking unescorted access to secure areas:

(1) Visually match the photograph on the TWIC to the person presenting the TWIC.

(2) Visually check the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(3) Visually verify that the expiration date on the face of the TWIC has not passed.

■ 7. Add § 101.525 to read as follows:

**§ 101.525 TWIC inspection requirements for Risk Group B.**

Owners or operators of vessels, facilities, or Outer Continental Shelf facilities subject to part 104, 105, or 106 of this subchapter that are assigned to Risk Group B in §§ 104.263, 105.253, or 106.258 of this subchapter must ensure that at all Maritime Security (MARSEC) Levels, prior to each entry, all persons seeking unescorted access to secure areas present their Transportation Worker Identification Credentials (TWICs) for inspection before being granted such unescorted access.

(a) Inspection must include—

(1) A visual match of the photograph on the TWIC to the person presenting the TWIC;

(2) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged; and

(3) A visual verification that the expiration date on the face of the TWIC has not passed.

(b) Nothing in this section shall be read to prohibit an owner or operator from implementing the TWIC requirements of a higher Risk Group for their vessel or facility.

■ 8. Add § 101.530 to read as follows:

**§ 101.530 TWIC inspection requirements for Risk Group C.**

Owners or operators of vessels or facilities subject to part 104 or 105 of this subchapter that are assigned to Risk Group C in §§ 104.263 or 105.253 of this subchapter must ensure that at all Maritime Security (MARSEC) Levels, prior to each entry, all persons seeking unescorted access to secure areas present their TWICs for inspection before being granted such unescorted access.

(a) TWIC inspection must include—

(1) A visual match of the photograph on the TWIC to the person presenting the TWIC;

(2) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged; and

(3) A visual verification that the expiration date on the face of the TWIC has not passed.

(b) Nothing in this section shall be read to prohibit an owner or operator from implementing the TWIC requirements of a higher Risk Group for their vessel or facility.

■ 9. Add § 101.535 to read as follows:

**§ 101.535 TWIC inspection requirements in special circumstances.**

Owners or operators of any vessel, facility, or Outer Continental Shelf (OCS) facility subject to part 104, 105, or 106 of this subchapter must ensure that a TWIC program is implemented as follows:

(a) If a person cannot present a Transportation Worker Identification Credential (TWIC) because it has been lost, damaged, or stolen, and the person has previously been granted unescorted access to secure areas and is known to have had a TWIC, the person may be granted unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if—

(1) The person has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);

(2) The person can present another identification credential that meets the requirements of § 101.515 of this part; and

(3) There are no other suspicious circumstances associated with the person's claim that the TWIC was lost, damaged, or stolen.

(b) If a person's fingerprints are not able to be read by a TWIC reader or Physical Access Control System (PACS) due to technology malfunction, poor fingerprint quality, or no fingerprint minutiae, the owner or operator may grant the person unescorted access to secure areas based on either of the following secondary authentication procedures:

(1) The owner or operator may require the person to provide their Personal Identification Number (PIN); or

(2) The owner or operator may require the person to present an alternative biometric that has been incorporated into the PACS.

(c) If a TWIC reader malfunctions, and a person seeking unescorted access to

secure areas has previously been granted such unescorted access and is known to have a TWIC, the person may be granted unescorted access to secure areas for a period of no longer than 7 consecutive calendar days. During that period, the owner or operator must perform the following inspections prior to each entry:

(1) A visual match of the photograph on the TWIC to the person presenting the TWIC.

(2) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(3) A visual verification that the expiration date on the face of the TWIC has not passed.

(d) If a person cannot present a TWIC for any other reason than those outlined in paragraph (a) of this section, the person must not be granted unescorted access to secure areas. The person must be under escort, at all times, while in a secure area.

(e) With the exception of persons granted access according to paragraph (a) of this section, all persons granted unescorted access to secure areas of a vessel, facility, or OCS facility must be able to produce their TWICs upon request from the Transportation Safety Administration, the Coast Guard, other authorized Department of Homeland Security representatives, or a Federal, State, or local law enforcement officer.

(f) There must be disciplinary measures in place to prevent fraud and abuse.

(g) Owners or operators must establish the frequency of the application of any security measures for access control in their approved security plans, particularly if these security measures are applied on a random or occasional basis.

(h) The vessel, facility, or OCS facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of other entities that interface with the vessel, facility, or OCS facility.

## PART 104—MARITIME SECURITY: VESSELS

■ 10. 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.

### § 104.105 [Amended]

■ 11. In § 104.105(d), remove the words ''this part'', and add, in their place, the words ''parts 101 and 104 of this subchapter''.

■ 12. Amend § 104.115 by removing paragraph (c), redesignating paragraph (d) as paragraph (c), and revising newly redesignated paragraph (c) to read as follows:

### § 104.115 Compliance.

* * * * *

(c) By (2 YEARS AFTER DATE OF PUBLICATION OF FINAL RULE), owners and operators of vessels subject to this part must amend their security plans, if necessary, to indicate how they will implement the TWIC reader requirements in this subchapter. By (2 YEARS AFTER DATE OF PUBLICATION OF FINAL RULE), owners and operators of Risk Group A vessels subject to this part must operate in accordance with the TWIC reader provisions found within this subchapter.

### § 104.200 [Amended]

■ 13. Amend § 104.200 as follows:

■ a. In paragraph (b)(12) introductory text, remove the word ''part'', and add, in its place, the word ''subchapter''; and

■ b. In paragraph (b)(14), remove the words ''§ 104.265(c) of this part'', and add, in their place, the words ''§ 101.535(a) of this subchapter''.

■ 14. Amend § 104.235 as follows:

■ a. In paragraph (b)(7), following the words ''of its effective period;'', remove the word ''and'';

■ b. In paragraph (b)(8), following the words ''the audit was completed'', remove the symbol ''.'' and add, in its place, the word ''; and'';

■ c. Add paragraph (b)(9); and

■ d. In paragraph (c), add a sentence to the end of the paragraph.

The additions read as follows:

### § 104.235 Vessel recordkeeping requirements.

* * * * *

(b) * * *

(9) *TWIC Reader/PACS.* For each individual granted unescorted access to a secure area, the: FASC–N; date and time that unescorted access was granted; and, if captured, the individual's name. Additionally, documentation to demonstrate that the owner or operator has updated the CCL with the frequency required in § 101.520 of this subchapter.

(c) * * * TWIC reader records and similar records in a PACS are sensitive security information and must be protected in accordance with 49 CFR part 1520.

■ 15. Add § 104.263 to read as follows:

### § 104.263 Risk Group classifications for vessels.

(a) For purposes of the Transportation Worker Identification Credential (TWIC) requirements of this subchapter, the following vessels subject to this part are in Risk Group A:

(1) Vessels that carry Certain Dangerous Cargoes (CDC) in bulk.

(2) Vessels certificated to carry more than 1,000 passengers.

(3) Towing vessels engaged in towing a barge or barges subject to paragraph (a)(1) or vessels subject to paragraph (a)(2) of this section.

(b) For purposes of the TWIC requirements of this subchapter, the following vessels subject to this part are in Risk Group B:

(1) Vessels that carry hazardous materials other than CDC in bulk.

(2) Vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues.

(3) Vessels certificated to carry 500 to 1,000 passengers.

(4) Towing vessels engaged in towing a barge or barges subject to paragraph (b)(1), (b)(2), or vessels subject to paragraph (b)(3) of this section.

(c) For purposes of the TWIC requirements of this subchapter, the following vessels subject to this part are in Risk Group C:

(1) Vessels carrying non-hazardous cargoes that are required to have a vessel security plan (VSP).

(2) Vessels certificated to carry less than 500 passengers.

(3) Towing vessels engaged in towing a barge or barges subject to paragraph (c)(1) or vessels subject to paragraph (c)(2) of this section.

(4) Mobile Offshore Drilling Units (MODUs).

(5) Offshore Supply Vessels (OSVs) subject to 46 CFR chapter I, subchapter L or I.

(d) Vessels may move from one Risk Group classification to another, based on the cargo they are carrying or handling at any given time. An owner or operator expecting a vessel to move between Risk Groups must explain, in the VSP, the timing of such movements, as well as how the vessel will move between the requirements of the higher and lower Risk Groups, with particular attention to the security measures to be taken when moving from a lower Risk Group to a higher Risk Group.

■ 16. Amend § 104.265 as follows:

■ a. Revise paragraph (a)(4);

■ b. Remove paragraphs (c) and (d);

■ c. Redesignate paragraphs (e) through (h) as paragraphs (c) through (f), respectively;

■ d. Revise newly redesignated paragraph (d)(1);

■ e. In newly redesignated paragraph (e)(6), remove the word ''and'';

■ f. In newly redesignated paragraph (e)(7), following the words ''cooperation

with the facility'', remove the symbol ''.'' and add, in its place, the word ''; and'';

■ g. Add paragraph (e)(8);

■ h. In newly redesignated paragraph (f)(9), remove the word ''or'';

■ i. In newly redesignated paragraph (f)(10), following the words ''search of the vessel'', remove the symbol ''.'' and add, in its place, the word ''; or''; and

■ j. Add paragraph (f)(11).

The revisions and additions read as follows:

**§ 104.265 Security measures for access control.**

(a) * * *

(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. Depending on a vessel's Risk Group, TWICs must be checked either visually or electronically using a TWIC reader or as integrated into a PACS at the locations where TWIC-holders embark the vessel.

* * * * *

(d) * * *

(1) Implement TWIC as set out in §§ 101.520, 101.525, or 101.530 of this subchapter, as applicable, and in accordance with the vessel's assigned Risk Group, as set out in § 104.263 of this part;

* * * * *

(e) * * *

(8) Implementing additional TWIC requirements, as required by § 104.263 of this part and §§ 101.520, 101.525, or 101.530 of this subchapter, if relevant.

* * * * *

(f) * * *

(11) Implementing additional TWIC requirements, as required by § 104.263 of this part and §§ 101.520, 101.525 or 101.530 of this subchapter, if relevant.

**§ 104.267 [Amended]**

■ 17. In § 104.267(a), remove the last sentence.

**§ 104.292 [Amended]**

■ 18. Amend § 104.292 as follows:

■ a. In paragraph (b) introductory text, remove the words ''(f)(2), (f)(4), and (f)(9)'' and add, in its place, the words ''(d)(2), (d)(4), and (d)(9)'';

■ b. In paragraph (e)(3), remove the words ''§ 104.265(f)(4) and (g)(1)'', and add, in their place, the words ''§ 104.265(d)(4) and (e)(1)''; and

■ c. In paragraph (f), remove the words ''§ 104.265(f)(4) and (h)(1)'', and add, in their place, the words ''§ 104.265(d)(4) and (f)(1)''.

■ 19. Amend § 104.405 as follows:

■ a. Revise paragraph (a)(10); and

■ b. In paragraph (b), remove the last sentence.

The revisions read as follows:

**§ 104.405 Format of the Vessel Security Plan (VSP).**

(a) * * *

(10) Security measures for access control, including the vessel's TWIC program, designated passenger access areas, and employee access areas;

* * * * *

## PART 105—MARITIME SECURITY: FACILITIES

■ 20. 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.

■ 21. Amend § 105.110 by revising paragraph (b) to read as follows:

**§ 105.110 Exemptions.**

* * * * *

(b) A public access area designated under § 105.106 is exempt from the requirements for screening of persons, baggage, and personal effects and identification of persons in §§ 101.520, 101.525, or 101.530 of this subchapter, as applicable, and § 105.255(c)(1), (c)(3), (d)(1), and (e)(1) and § 105.285(a)(1).

* * * * *

■ 22. Amend § 105.115 as follows:

■ a. In paragraph (c), following the words ''§ 105.415 of this part'', remove the words '', by September 4, 2007''; and

■ b. Remove paragraph (d), redesignate paragraph (e) as paragraph (d), and revise newly redesignated paragraph (d) to read as follows:

**§ 105.115 Compliance.**

* * * * *

(d) By (2 YEARS AFTER DATE OF PUBLICATION OF FINAL RULE), owners and operators of facilities subject to this part must amend their security plans, if necessary, to indicate how they will implement the TWIC reader requirements in this subchapter. By (2 YEARS AFTER DATE OF PUBLICATION OF FINAL RULE), owners and operators of Risk Group A facilities subject to this part must be operating in accordance with the TWIC reader provisions found within this subchapter.

**§ 105.200 [Amended]**

■ 23. Amend § 105.200 as follows:

■ a. In paragraph (b)(6) introductory text, remove the word ''part'', and add, in its place, the word ''subchapter''; and

■ b. In paragraph (b)(15), remove the words ''section 105.255(c) of this part'', and add, in their place, the words ''§ 101.535(a) of this subchapter''.

■ 24. Amend § 105.225 as follows:

■ a. In paragraph (b)(7), following the words ''of its effective period;'', remove the word ''and'';

■ b. In paragraph (b)(8), following the words ''the audit was completed'', remove the symbol ''.'' and add, in its place, the word ''; and'';

■ c. Add paragraph (b)(9); and

■ d. In paragraph (c), add a sentence to the end of the paragraph.

The additions read as follows:

**§ 105.225 Facility recordkeeping requirements.**

* * * * *

(b) * * *

(9) *TWIC Reader/PACS.* For each individual granted unescorted access to a secure area, the: FASC–N; date and time that unescorted access was granted; and, if captured, the individual's name. Additionally, documentation to demonstrate that the owner or operator has updated the CCL with the frequency required in § 101.520 of this subchapter.

(c) * * * TWIC reader records and similar records in a PACS are sensitive security information and must be protected in accordance with 49 CFR part 1520.

■ 25. Add § 105.253 to read as follows:

**§ 105.253 Risk Group classifications for facilities.**

(a) For purposes of the Transportation Worker Identification Credential (TWIC) requirements of this subchapter, the following facilities subject to this part are in Risk Group A:

(1) Facilities that handle Certain Dangerous Cargoes (CDC) in bulk.

(2) Facilities that receive vessels certificated to carry more than 1,000 passengers.

(3) Barge fleeting facilities that receive barges carrying CDC in bulk.

(b) For purposes of the TWIC requirements of this subchapter, the following facilities subject to this part are in Risk Group B:

(1) Facilities that receive vessels that carry hazardous materials other than CDC in bulk.

(2) Facilities that receive vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues.

(3) Facilities that receive vessels certificated to carry 500 to 1,000 passengers.

(4) Facilities that receive towing vessels engaged in towing a barge or barges carrying hazardous materials other than CDC in bulk, crude oil, or towing vessels certificated to carry 500 to 1,000 passengers.

(c) For purposes of the TWIC requirements of this subchapter, the following facilities subject to this part are in Risk Group C:

(1) Facilities that receive vessels carrying non-hazardous cargoes not otherwise included in paragraph (a) or (b) of this section.

(2) Facilities that receive vessels certificated to carry less than 500 passengers.

(3) Facilities that receive towing vessels engaged in towing a barge carrying non-hazardous cargoes or less than 500 passengers.

(d) Facilities may move from one Risk Group classification to another, based on the material they handle or the types of vessels they receive at any given time. An owner or operator of a facility expected to move between Risk Groups must explain, in the facility security plan, the timing of such movements, as well as how the facility will move between the requirements of the higher and lower Risk Groups, with particular attention to the security measures to be taken when moving from a lower Risk Group to a higher Risk Group.

■ 26. Amend § 105.255 as follows:

■ a. Revise paragraph (a)(4);

■ b. Remove paragraphs (c) and (d);

■ c. Redesignate paragraphs (e) through (h) as paragraphs (c) through (f), respectively;

■ d. Revise newly redesignated paragraph (d)(1);

■ e. In newly redesignated paragraph (c), remove the words ''Facility Security Plan (FSP)'' and add, in their place, the word ''FSP''.

■ f. In newly redesignated paragraph (e)(6), remove the word ''or'';

■ g. In newly redesignated paragraph (e)(7), following the words ''in the approved FSP'', remove the symbol ''.'' and add, in its place, the word ''; or'';

■ h. Add paragraph (e)(8);

■ i. In newly redesignated paragraph (f)(8), remove the word ''or'';

■ j. In newly redesignated paragraph (f)(9), following the words ''within the facility'', remove the symbol ''.'' and add, in its place, the word ''; or''; and

■ k. Add paragraph (f)(10) as follows:

The revisions and additions read as follows:

**§ 105.255 Security measures for access control.**

(a) * * *

(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. Depending on a facility's Risk Group, TWICs must be inspected either visually or electronically using a TWIC reader or as integrated into a PACS at the access points to the secure areas designated in the facility security plan (FSP).

* * * * *

(d) * * *

(1) Implement TWIC as set out in §§ 101.520, 101.525, or 101.530 of this subchapter, as applicable, and in accordance with the facility's assigned Risk Group, as set out in § 105.253 of this part;

* * * * *

(e) * * *

(8) Implementing additional TWIC requirements, as required by § 105.253 of this part and §§ 101.520, 101.525, or 101.530 of this subchapter, if relevant.

* * * * *

(f) * * *

(10) Implementing additional TWIC requirements, as required by § 105.253 of this part and § 101.520, 101.525, or 101.530 of this subchapter, if relevant.

**§ 105.257 [Amended]**

■ 27. In § 105.257(a), remove the last sentence.

■ 28. Revise § 105.290(b) to read as follows:

**§ 105.290 Additional requirements—cruise ship terminals.**

* * * * *

(b) Check the identification of all persons seeking to enter the facility. Persons holding a TWIC shall be checked as set forth in §§ 101.520, 101.525 or 101.530 of this subchapter, as applicable, in accordance with the facility's assigned Risk Group, as set out in § 105.253 of 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;

* * * * *

■ 29. Revise § 105.296(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 §§ 101.520, 101.525 or 101.530 of this subchapter, as applicable, in accordance with the facility's assigned Risk Group, as set out in § 105.253 of this part.

* * * * *

■ 30. Amend § 105.405 as follows:

■ a. Revise paragraph (a)(10); and

■ b. In paragraph (b), remove the last sentence.

The revisions read as follows:

**§ 105.405 Format and content of the Facility Security Plan (FSP).**

(a) * * *

(10) Security measures for access control, including the facility's TWIC program and designated public access areas;

* * * * *

## PART 106—MARINE SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

■ 31. 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.

**§ 106.110 [Amended]**

■ 32. In § 106.110, remove paragraphs (d) and (e).

**§ 106.200 [Amended]**

■ 33. Amend § 106.200 as follows:

■ a. In paragraph (b)(6) introductory text, remove the word ''part'', and add, in its place, the word ''subchapter''; and

■ b. In paragraph (b)(12), remove the words ''§ 106.260(c) of this part'', and add, in their place, the words ''§ 101.535 of this subchapter''.

■ 34. Add § 106.258 to read as follows:

**§ 106.258 Risk Group classifications for OCS facilities.**

For purposes of the Transportation Worker Identification Credential requirements of this subchapter, all Outer Continental Shelf facilities subject to this part are classified in Risk Group B.

■ 35. Amend § 106.260 as follows:

■ a. Remove paragraphs (c) and (d);

■ b. Redesignate paragraphs (e) through (h) as paragraphs (c) through (f), respectively;

■ c. Revise newly redesignated paragraph (d)(1);

■ d. In newly redesignated paragraph (e)(3), remove the word ''or'';

■ e. In newly redesignated paragraph (e)(4), following the words ''providing boat patrols'', remove the symbol ''.'' and add, in its place, the word ''; or'';

■ f. Add paragraph (e)(5);

■ g. In newly redesignated paragraph (f)(7), remove the word ''or'';

■ h. In newly redesignated paragraph (f)(8), following the words ''search of the OCS facility'', remove the symbol ''.'' and add, in its place, the word ''; or''; and

■ i. Add paragraph (f)(9).

The revisions and additions read as follows:

**§ 106.260 Security measures for access control.**

* * * * *

(d) * * *

(1) Implement TWIC as set out in § 101.525 of this subchapter in

accordance with the OCS facility's assigned Risk Group, as set out in § 106.258 of this part.

* * * * *

(e) * * *

(5) Implementing additional TWIC requirements, as required by § 106.258 of this part and § 101.525 of this subchapter.

* * * * *

(f) * * *

(9) Implementing additional TWIC requirements, as required by § 106.258 of this part and § 101.525 of this subchapter.

**§ 106.262 [Amended]**

■ 36. In § 106.262(a), remove the last sentence.

■ 37. Amend § 106.405 as follows:

■ a. Revise paragraph (a)(10); and

■ b. In paragraph (b), remove the last sentence.

The revisions read as follows:

**§ 106.405 Format of the Facility Security Plan (FSP).**

(a) * * *

(10) Security measures for access control, including the OCS facility's TWIC program;

* * * * *

Dated: March 13, 2013.

**Admiral Robert J. Papp Jr.,**

*Commandant, U.S. Coast Guard.*

[FR Doc. 2013–06182 Filed 3–21–13; 8:45 am]

BILLING CODE 9110–04–P