**DEPARTMENT OF HOMELAND SECURITY**

**Coast Guard**

**33 CFR Parts 101, 103, 104, 105 and 106**

**[Docket No. USCG–2007–28915]**

**RIN 1625–AB21**

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

**AGENCY:** Coast Guard, DHS.

**ACTION:** Final rule.

**SUMMARY:** The Coast Guard is issuing a final rule to require owners and operators of certain vessels and facilities regulated by the Coast Guard to conduct electronic inspections of Transportation Worker Identification Credentials (TWICs) as an access control measure. This final rule also implements recordkeeping requirements and security plan amendments that would incorporate these TWIC requirements. The TWIC program, including the electronic inspection requirements in this final rule, is an important component of the Coast Guard's multi-layered system of access control requirements designed to enhance maritime security.

This rulemaking action builds upon existing regulations designed to ensure that only individuals who hold a valid TWIC are granted unescorted access to secure areas of Coast Guard-regulated vessels and facilities. The Coast Guard and the Transportation Security Administration have already promulgated regulations pursuant to the Maritime Transportation Security Act that require mariners and other individuals to hold a TWIC prior to gaining unescorted access to a secure area. By requiring certain high-risk vessels and facilities to perform electronic TWIC inspections, this rule enhances security at those locations. This rule also implements the Security and Accountability For Every Port Act of 2006 electronic reader requirements.

**DATES:** This final rule is effective August 23, 2018.

**ADDRESSES:** Comments and materials received from the public, as well as documents mentioned in this preamble as being available in the docket, are part of docket USCG–2007–28915 and are available using the Federal eRulemaking Portal. You can find this docket on the Internet by going to *http://www.regulations.gov,* entering ''USCG–2007–28915'' and then clicking ''Search.''

**FOR FURTHER INFORMATION CONTACT:** For information about this document, call or email LCDR Kevin McDonald, Coast Guard; telephone 202–372–1168, email *Kevin.J.Mcdonald2@uscg.mil.*

**SUPPLEMENTARY INFORMATION:**

### Table of Contents for Preamble



## I. Abbreviations

AHP—Analytical Hierarchy Process
ANPRM—Advanced Notice of Proposed Rulemaking
ASP—Alternative Security Program
CCA—Certificate for Card Authentication
CCL—Canceled Card List
CCTV—Closed-Circuit Television
CDC—Certain Dangerous Cargoes
CFR—Code of Federal Regulations
CHUID—Card Holder Unique Identifier
COI—Certificate of Inspection
DHS—Department of Homeland Security
DRAA—Designated Recurring Access Area
E.O.—Executive Order
FASC—N Federal Agency Smart Credential—Number
FR—Federal Register
FSP—Facility Security Plan
ICE—Initial Capability Evaluation
MARSEC—Maritime Security
MISLE—Marine Information for Safety and Law Enforcement
MSRAM—Maritime Security Risk Analysis Model
MTSA—Maritime Transportation Security Act of 2002
NIST—National Institute of Standards and Technology
NPRM—Notice of Proposed Rulemaking
NTTAA—National Technology Transfer and Advancement Act
NVIC—Navigation and Vessel Inspection Circular
OCS—Outer Continental Shelf
OMB—Office of Management and Budget
PAC—Policy Advisory Council
PACS—Physical Access Control System
PVA—Passenger Vessel Association
PII—Personal Identifying Information
PIN—Personal Identification Number
Pub. L.—Public Law
QTL—Qualified Technology List
RA—Regulatory Analysis
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
U.S.C.—United States Code
VSP—Vessel Security Plan

## II. Regulatory History and Information

On May 22, 2006, the Coast Guard and the Transportation Security Administration (TSA) jointly published a Notice of Proposed Rulemaking (NPRM) entitled ''Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License.'' [1] On January 25, 2007, the Coast Guard and TSA published the final rule, also entitled ''Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License.'' [2]

Although the May 22, 2006 NPRM proposed certain TWIC reader requirements, after reviewing the public comments, the Coast Guard decided to remove the proposed TWIC reader requirements from the January 25, 2007 final rule, address them in a separate rulemaking, and conducted a pilot program to address the feasibility of reader requirements before issuing a final rule.[3] For a detailed discussion of those public comments and Coast Guard responses, please refer to the January 25, 2007 final rule.[4]

On March 27, 2009, the Coast Guard published an Advanced Notice of Proposed Rulemaking (ANPRM) for this rulemaking.[5] On March 22, 2013, the Coast Guard published the NPRM for this rulemaking.[6] Additionally, we held four public meetings across the country in 2013.

## III. Executive Summary

### *A. Basis and Purpose*

In accordance with the Maritime Transportation Security Act of 2002 (MTSA) and the Security and Accountability For Every Port Act of 2006 (SAFE Port Act), the Coast Guard is establishing rules requiring electronic readers for use at high-risk vessels and at facilities. These rules will ensure that prior to being granted unescorted access to a designated secure area, an individual will have his or her TWIC authenticated, the status of that credential validated against an up-to-date list maintained by the TSA, and the individual's identity confirmed by comparing his or her biometric (*i.e.* fingerprint) with a biometric template stored on the credential. By promulgating these rules, the Coast Guard is complying with the statutory requirement in the SAFE Port Act, improving security at the highest risk maritime transportation-related vessels and facilities, and making full use of the electronic and biometric security features integrated into the TWIC and mandated by Congress in MTSA.

The TWIC is currently being used as a visual identity badge on many vessels and facilities. Essentially, DHS requires that a security guard examines the security features (hologram and watermark) embedded on the surface of the credential, checks the expiration date listed on the card, and compares the photograph to the person presenting the credential. While this system of ''visual TWIC inspection'' provides some benefits, it does not address all security concerns, nor does it make full use of the security features contained in the TWIC. For example, if a TWIC is stolen or lost, an unauthorized individual could make use of the credential, and provided that individual resembles the picture on the TWIC, could gain access to a secure area. Additionally, if a TWIC is revoked because the individual has committed a disqualifying offense, such as the theft of explosives, there is no way for security officers on a vessel or at a facility to determine that fact from the face of the TWIC. Finally, a sophisticated adversary could forge a realistic replica of a credential. It is also worth noting that since a TWIC-holder is required to renew his or her credential every 5 years, the TWIC-holder's resemblance to the picture on the TWIC may decrease over time, rendering visual inspection a somewhat less accurate means to confirm identity. Through the process of ''electronic TWIC inspection,'' by which TWICs are authenticated, validated, and the individual's identity confirmed biometrically, all of these scenarios would be thwarted or mitigated.

In this rulemaking process, the Coast Guard published an ANPRM, published an NPRM, hosted a series of public meetings around the country to solicit public input, and worked with the Transportation Security Administration to conduct a pilot program. As a result of this input, the Coast Guard made a number of changes and clarifications in this final rule that we believe provide a robust system that improves security, addresses industry, labor, and Congressional concerns, and clarifies numerous issues relating to the operational nature of the electronic TWIC inspection program. Primarily, this rule allows for an even more flexible implementation of the electronic TWIC inspection requirements than the proposed rule that will allow new systems to be integrated into existing security and access control systems. We believe that this flexibility will provide robust security without causing unnecessary costs or significantly disrupting business operations. A brief summary of the main changes from the proposed rule to the final rule follows.

- This final rule provides additional flexibility with regard to the purchase, installation, and use of electronic readers. Instead of requiring the use of a TWIC reader on the TSA's Qualified Technology List (QTL), owners and operators can choose to fully integrate electronic TWIC inspection and biometric matching into a new or existing Physical Access Control System (PACS).
- We clarify that this final rule only affects Risk Group A vessels and facilities, and that no changes to the existing business practices of other MTSA-regulated vessels and facilities are required.
- This final rule eliminates the distinction between Risk Groups B and C for both vessels and facilities. If and when a requirement for electronic TWIC inspection may be considered for MTSA-regulated vessels and facilities not currently in Risk Group A, we will provide an updated analysis of the costs and benefits of such an action and define new Risk Groups accordingly.
- This final rule clarifies that for Risk Group A facilities, electronic TWIC inspection is required each time a person is granted unescorted access to a secure area (a limited exception is permitted for Recurring Unescorted Access, or RUA). For Risk Group A vessels, electronic TWIC inspection is only required when boarding the vessel, even if only parts of the vessel are considered secure areas.
- This final rule eliminates the special requirement that barge fleeting facilities that handle or receive barges carrying Certain Dangerous Cargoes (CDC) in bulk be classified as Risk Group A. Barge fleeting facilities are instead classified the same as all other facilities. This change will effectively eliminate most isolated barge facilities

[1] 71 FR 29396.

[2] 72 FR 3492.

[3] The TWIC Reader Pilot was established pursuant to Section 104 of the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) (P.L. 109–347), which was codified at 46 U.S.C. 70105 (k)(4).

[4] 72 FR 3511.

[5] 74 FR 13360.

[6] 78 FR 17782.

from the electronic TWIC inspection requirements due to a lack of a secure area.

- This final rule increases the exemption from electronic TWIC inspection requirements to vessels with 20 or fewer TWIC-holding crewmembers and defines that number as the minimum manning requirement specified on a vessel's Certificate of Inspection.
- This final rule provides additional flexibility for ferries and other vessels that use dedicated terminals in Risk Group A to integrate their electronic TWIC inspection programs with their terminals' programs.

*B. Summary of Costs and Benefits*

Of the approximately 13,825 vessels, 3,270 facilities, and 56 Outer Continental Shelf (OCS) facilities regulated by MTSA, this final rule impacts only certain ''Risk Group A'' vessels and facilities, which currently number 1 vessel [7] and 525 facilities under the revised applicability definitions for the final rule. No OCS facilities are affected by this final rule. We estimate the annualized cost of this final rule to be approximately $22.5 million, while the 10-year cost is $157.9 million, discounted at 7 percent. The main cost drivers of this rule are the acquisition, installation, and integration of TWIC readers into access control systems. Annual costs will be driven by costs associated with updates of the list of cancelled TWICs, recordkeeping, training, system maintenance, and opportunity costs associated with failed TWIC reader transactions. The estimated annualized cost of this final rule discounted at 7 percent is approximately $5.1 million less than the estimated cost of the NPRM.

The benefits of this final 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. The main benefit of this regulation, decreased risk of a Transportation Security Incident (TSI), cannot be quantified given current data limitations. We used a risk-based approach to apply these regulatory requirements to less than 5 percent of the MTSA-regulated population, which represents approximately 80 percent of the potential consequences of a TSI. The provisions in this final rule target the highest risk entities while maximizing the net benefits of the rule.

Table 1 provides the estimated costs and functional benefits associated with the requirements of the TWIC reader.

TABLE 1—ESTIMATED COSTS AND FUNCTIONAL BENEFITS OF TWIC READER REQUIREMENTS

| Category | Final Rule |
|---|---|
| Applicability | High-risk MTSA-regulated facilities and high risk MTSA-regulated vessels with greater than 20 TWIC-holding crewmembers. |
| Affected Population | 1 vessel.<br>525 facilities. |
| Costs ($ millions, 7% discount rate) | $22.5 (annualized).<br>$157.9 (10-year). |
| Costs (Qualitative) | Time to retrieve or replace lost PINs for use with TWICs. |
| Benefits (Qualitative) | Enhanced access control and security at U.S. maritime facilities and on board U.S.-flagged vessels.<br>Reduction of human error when checking identification and manning access points. |

For a more detailed discussion of costs and benefits, see the full Final Regulatory Analysis and Final Regulatory Flexibility Analysis available in the online docket for this rulemaking. Appendix G of that document outlines the costs by provision and also discusses the complementary nature of the provisions.

## IV. Background

The MTSA provides a multi-layered approach to maritime security which includes measures to consider broader security issues at U.S. ports and waterways, the coastal zone, the open ocean, and foreign ports. Under this multi-layered system, the Coast Guard is authorized to regulate vessels and facilities, and 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 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 reports; and (18) TWIC procedures.[8]

For the 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.'' [9] For the 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.'' [10] Coast Guard regulations implementing MTSA with respect to vessels [11] apply to: Mobile Offshore Drilling Units, cargo vessels, or passenger vessels subject to the 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

[7] We note that the number of vessels affected by the provision is low, as most ''Risk Group A'' vessels are exempt from the electronic TWIC inspection requirements due to a low crewmember count.

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

[9] 46 U.S.C. 70101(2).

[10] 46 U.S.C. 115; 1 U.S.C. 3.

[11] *See* 33 CFR 104.105(a).

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 CDC; [12] barges carrying CDC or cargo and miscellaneous vessels engaged on an international voyage; tank ships; and generally, towing vessels greater than 8 meters in register length engaged in towing barges.

TWIC requirements in those regulations do not apply to: Foreign vessels; mariners employed aboard vessels moored at U.S. facilities only when they are working immediately adjacent to their vessels in the conduct of vessel activities; except pursuant to international treaty, convention, or agreement to which the U.S. is a party, to any foreign vessel that is not destined for, or departing from, a port or place subject to the jurisdiction of the U.S. and that is either (a) in innocent passage through the territorial sea of the U.S., or (b) in transit through the navigable waters of the U.S. that form a part of an international strait.[13]

Coast Guard regulations implementing MTSA with respect to facilities [14] 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 CDC; 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.

Those regulations do not apply to: A facility owned or operated by the U.S. that is used primarily for military purposes; an oil and natural gas production, exploration, or development facility regulated by 33 CFR parts 126 or 154 if (a) the facility is engaged solely in the exploration, development, or production of oil and natural gas, and (b) the facility does not meet or exceed the operating conditions in 33 CFR 106.105; a facility that supports the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 if (a) the facility is engaged solely in the support of exploration, development, or production of oil and natural gas and transports or stores quantities of hazardous materials that do not meet or exceed those specified in 49 CFR 172.800(b)(1) through (b)(6), or (b) the facility stores less than 42,000 gallons of cargo regulated by 33 CFR part 154; a mobile facility regulated by 33 CFR part 154; or an isolated facility that receives materials regulated by 33 CFR parts 126 or 154 by vessel due to the lack of road access to the facility and does not distribute the material through secondary marine transfers.[15] Additionally, the TWIC requirements in those regulations do not apply to mariners employed aboard vessels moored at U.S. facilities only when they are working immediately adjacent to their vessels in the conduct of vessel activities.[16]

This rulemaking applies to the above-described vessels and facilities regulated by the Coast Guard pursuant to the authority granted in MTSA, and will further increase the security value of TWIC to the nation by making use of the statutorily-mandated biometric identification function and other security features. A complete statutory and regulatory history of this rulemaking can be found in Section III.B of the NPRM published on March 22, 2013.[17]

The TWIC program falls under the access control requirements as one component of MTSA. Since April 15, 2009, the TWIC has been used throughout the maritime sector for access to secure areas of MTSA-regulated facilities and vessels. Its purpose is to ensure a vetted maritime workforce by establishing security-related eligibility criteria, and by requiring each TWIC-holder to undergo a security threat assessment from the TSA 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 PIN, 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) card authentication, (2) card validation, and (3) identity verification.

Card authentication ensures that the TWIC is not counterfeit. Security personnel can authenticate a TWIC by visually inspecting the security features on the card. An electronic reader provides enhanced authentication by performing a challenge/response protocol using the Certificate for Card Authentication (CCA) and the associated card authentication private key stored in the TWIC. The electronic reader will read the CCA 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 electronic reader). The electronic reader software will use the public key embedded in the CCA to verify that the signature of the random data block returned by the TWIC is valid. If the signature is valid, the electronic reader will trust the TWIC submitted and will then pull the FASC–N and other information from the card for further processing. The CCA contains the FASC–N and a certificate expiration date harmonized to the TWIC expiration date. This minimizes the need for the electronic reader to pull more information from the TWIC (unless required for additional checking).

The card validity check ensures that the TWIC has not expired or been cancelled 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. Currently, a TSA-canceled TWIC is placed on TSA's official CCL, which is updated daily. TSA's CCL is available online at: *https://universalenroll.dhs.gov/.* Currently, the process of TWIC visual inspection does not require the security guard to compare the cardholder's name to the CCL and therefore facilities do not know when specific card holders have had their credentials cancelled and may continue to grant access unknowingly. Using an electronic reader, card validity is further 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 PACS.

Identity verification entails comparing the individual presenting the TWIC to 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 an electronic reader, identity can be

[12] 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.

[13] *See* 33 CFR 104.105(d)–(f).

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

[15] *See* 33 CFR 105.105(c).

[16] *See* 33 CFR 105.105(d) and 106.105(b).

[17] 78 FR 17789.

verified by matching one of the biometric templates stored in the TWIC to the TWIC-holder's live sample biometric, matching to the PACS enrolled reference biometrics linked to the FASC–N of the TWIC, or requiring the TWIC-holder to place the TWIC into a TWIC reader (currently a PIN can only be accessed using a TWIC reader with a contact interface) and entering their PIN to release the digital facial image from the TWIC. This avoids the vulnerabilities of visual inspection by using the biometric capabilities mandated by Congress.

## V. Discussion of Comments and Changes to the Final Rule

In response to publication of the March 22, 2013 NPRM, the Coast Guard received over 100 comment letters, consisting of over 1,200 unique comments. Commenters provided numerous opinions, arguments, questions, and recommendations regarding the proposed TWIC reader requirements. In this section, we describe the comments received, as well as how they influenced the decisions made in this final rule. Overall, we have grouped our discussion into five sections, as discussed below.

In Section A, we address comments relating to the TWIC program generally, and electronic TWIC inspection specifically. This section includes comments relating to what the program's purpose is, how it affects security, and how it is tailored to achieve these goals in the most cost-effective and least-burdensome manner. We also discuss the risk analysis methodology in this section, in order to address comments relating to the specific types of threats the electronic TWIC inspection program is designed to combat.

Sections B through D of this discussion respond to comments relating to the operational aspects of the electronic TWIC inspection program. Most comments received were of a practical nature, especially those asking for clarifications on exactly how the regulations would apply in a large variety of specific situations. Section B addresses the specific nature of what an ''electronic TWIC inspection'' is, including what must be carried out, how such an inspection can be carried out using a PACS, recordkeeping requirements arising from electronic TWIC inspections, and how specific problems, such as a misplaced TWIC, would be addressed in the regulations.

Section C addresses when an electronic TWIC inspection must take place, including the specific locations on a facility or vessel where electronic readers must be located, and the parameters of an RUA configuration. Section D responds to comments relating to the classification of vessels and facilities into Risk Groups, including questions relating to barge fleeting facilities, shifting Risk Groups, and the exemption from electronic TWIC inspection requirements for vessels with a low number of crewmembers.

Items relating to the economic issues of electronic TWIC inspection are addressed in Section E. Comments on these issues related to the costs of TWIC readers, throughput times for TWIC transactions, and potential changes in security staffing needs.

Finally, Section F addresses several miscellaneous issues. Primary among these issues are comments relating to the TWIC Pilot Program and the Government Accountability Office (GAO) report on TWIC readers, issued in 2013 shortly before publication of the NPRM and accompanying analysis.[18] Additionally, this section addresses all other comments and questions that were not included in other sections.

### *A. General Matters Relating to TWIC*

In response to the NPRM, the Coast Guard received a large variety of comments relating to the TWIC program. In this section, we begin with those comments that address the TWIC program as a whole. Multiple commenters expressed dissatisfaction with the TWIC program as a whole and suggested that it be dismantled. Many of these commenters noted that specific facilities or vessels had not been targeted by terrorists, and argued that the costs of the program were unnecessary. For a variety of reasons described extensively throughout this document, we believe that the targeted measures established in this final rule provide a cost-effective mitigation of various threats that could result in a TSI. For example, in the Regulatory Analysis (RA), we describe three hypothetical yet plausible scenarios in which an individual could gain access to a vessel or facility using a forged or stolen TWIC,[19] threats that could specifically be reduced by electronic TWIC inspection. Congress has mandated, and we agree, that preventing unauthorized individuals from accessing secure areas of the nation's transportation infrastructure is part of a necessary security program. While we also agree with many commenters who suggested that it does not prevent every possible security threat, that is not the purpose of this final rule. The purpose of this final rule is to improve security at the highest risk maritime transportation-related vessels and facilities through the use of an electronic reader.

One commenter criticized the Maritime Security Risk Analysis Model (MSRAM) threat analysis methodology, because it did not address the security issues raised by cargo containers, which include the potential for concealed threats within the containers. While we note that MSRAM does include scenarios associated with threats from cargo containers, for the purposes of the current analysis of electronic TWIC inspection, we limited our consideration to attack scenarios that require physical proximity to the intended target and for which access control would affect the ability to conduct an attack. Controlling access to a target is an essential component of security from such attacks because access control helps to detect and perhaps interdict or at least delay the attackers before they reach the target. TWIC readers enhance the reliability of access control measures, thereby increasing the likelihood of identifying and denying/delaying access to an individual or group attempting nefarious acts. For this reason, our analysis in this final rule focuses on threats that could be prevented or mitigated through use of electronic TWIC inspection. Concealed items or persons smuggled inside cargo containers are not attack scenarios that transportation worker identity verification (and electronic TWIC inspection in particular) addresses. Therefore, analyzing those scenarios would not be useful for this rule. Coast Guard regulations address security measures for those attack scenarios in other ways. Vessel and facility security plans must describe in detail how they meet all relevant security requirements, including the security measures in place for handling cargo.[20]

Multiple commenters expressed concern over the application process for obtaining a new or renewal TWIC, stating that delays have saddled workers with an undue burden. The Coast Guard understands the challenges encountered during the initial implementation of TWIC, and during the more recent surge of renewals. We note the progress that has been made in the TWIC application process since publication of the NPRM.

[18] ''Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed'' (GAO–13–198).

[19] RA, p. 88.

[20] *See* 33 CFR 104.405; 33 CFR 105.405; 33 CFR part 104, subpart B; and 33 CFR part 105, subpart B.

Furthermore, we note that comments relating to the card application process are outside the scope of this rulemaking, which pertains to electronic TWIC inspection requirements only.

One commenter sought clarification as to why the TWIC was not an acceptable form of identification for entry to U.S. Navy or Coast Guard bases, and stated that the TWIC should be recognized by the agency that is requiring its use within the maritime sector. This comment is also outside the scope of this rulemaking as it does not address TWIC readers or their application to maritime rather than Federal facilities (*e.g.,* Coast Guard or Navy military bases).

One commenter expressed concern with requiring electronic readers on vessels, stating that anyone boarding a vessel would need to first pass through a facility. The same commenter stated that seafarers should not be prevented from taking shore leave, and suggested that additional regulations be put in place to avoid unlawful charges to seafarers to transit facilities for shore leave. The Coast Guard understands these concerns and has applied this rulemaking to those vessels presenting the highest risk and to those vessels which, in most cases, will regularly visit international ports not regulated under MTSA. Additionally, Congress mandated seafarers' access in section 811 of the Coast Guard Authorization Act of 2010. This mandate requires each Facility Security Plan to ''provide a system for seamen assigned to a vessel at that facility, pilots, and representatives of seamen's welfare and labor organizations to board and depart the vessel through the facility in a timely manner at no cost to the individual.'' [21] The Coast Guard is currently conducting a separate rulemaking to implement section 811.[22]

Several commenters requested more flexibility within this final rule rather than a ''one size fits all'' approach. This final rule incorporates additional flexibility for vessel and facility operators in direct response to comments in which specific requests for flexibility were made. The Coast Guard wholly agrees that there is no ''one size fits all'' approach for maritime security given the vast range of facility and vessel operations which, in many cases, overlap or occur in close proximity to each other. This final rule moves to a more performance-based approach by defining the criteria for electronic inspection requirements that meet the TWIC access control measures. Additionally, this rule sets flexible baseline requirements for electronic reader implementation for those vessels and facilities. We believe that the increased flexibility will decrease the burden on industry by allowing the use of existing systems with minor modifications, increasing the pool of available electronic reader technology, and allowing the individual operators to determine the approach to meet the regulatory requirement that best facilitates their business needs.

Some commenters suggested that the TWIC should be a standardized credential that can be used at multiple facilities, and that having this Federal credential should be a standard credential, rather than requiring truck drivers and others who need access to secure areas to obtain individual site-specific badges. The commenters argued that the use of the credential could alleviate redundant and overlapping background checks for workers, such as drivers, that access multiple facilities. We partially agree with this argument, but believe we should elaborate more closely on the role that TWIC and other identification credentials play in ensuring security at maritime facilities. We disagree with the suggestion that the TWIC should be used as an ''all-access'' credential that would override the property rights and security responsibilities of vessel and facility owners. We believe (like many other commenters), that possession of TWIC should not automatically grant an individual access to secure areas because the mere possession of a TWIC does not entitle the holder to access another person's property. The decision to grant access to a secure area of a vessel or facility appropriately lies with the owner or operator of that vessel or facility. We expect vessel and facility operators to limit access to their secure spaces to those who need such access, and to ensure that only those with a valid TWIC are granted unescorted access.

However, we note that controlling access to facilities can be carried out in several ways. For example, a facility may grant unescorted access to employees who enter the facility multiple times per day on a regular basis, and also grant access to truck or bus drivers who may only enter the facility on an occasional basis. Such a facility may use different ways to control access, and ensure that all individuals granted unescorted access possess a valid TWIC. The facility may vary how it does this depending on the operator's business needs and on the reasons why different individuals are requesting unescorted access. In this example, the facility might have one entrance for employees who use a PACS card to enter secure areas of the facility, and have another entrance for truck or bus drivers, who would present a TWIC for inspection. A single access point could also contain both a PACS reader and a TWIC reader, the latter for use by contractors or visitors who may not have been issued a facility-specific access card.

In this final rule we have granted flexibility that allows operators to use a variety of means to grant unescorted access, including the use of the TWIC as a means of identification. However, this final rule does not require operators to grant unescorted access to any TWIC-holder. As is currently the case, access to any vessel or facility is granted by the owner or operator, who has the authority and responsibility to determine if the individual requesting access has a legitimate business purpose.

1. Purpose and Efficacy of the TWIC Program

Several commenters questioned the overall efficacy of the TWIC program, questioning whether the program, with or without electronic readers, does anything to improve security. The Coast Guard understands that there have been many challenges with the implementation of the TWIC program, but does believe that TWIC has improved access control at vessels and at maritime facilities across the country. The TWIC program's single standard and nationwide recognition is intended to ensure a secure, consistent biometrically enabled credential, and facilitate an efficient, resilient, mobile transportation workforce during routine and emergency situations. However, an individual successfully obtaining a TWIC is only the first half of a two-part process. First, vessel and facility security personnel must determine that an individual possesses a valid TWIC, meaning that they have been vetted. Second, they must verify the individual's authorization for entering a vessel or facility before granting the person unescorted access. As mentioned above, the mere possession of a valid TWIC alone is not sufficient to gain the holder of that credential access to secure areas on vessels or facilities across the country. The TWIC provides a means by which a vessel or facility security officer can determine that an individual has been vetted to an established and accepted standard. This determination

[21] *See* the Seafarers' Access to Maritime Facilities Notice of Proposed Rulemaking (79 FR 77981, 77985 (Dec. 29, 2014)).

[22] The docket for the Seafarers' Access rulemaking is available online at *www.regulations.gov* by entering ''USCG–2013–1087'' in the Search box.

helps inform the vessel or facility security officer's decision to grant unescorted access to an individual. Vessel and facility personnel may then evaluate a TWIC-holder's authorization and determine whether the TWIC-holder should be granted unescorted access.

One commenter took issue with a statement in the NPRM that read ''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.'' [23] The commenter stated that TWIC readers can identify cards that were obtained through unreported theft of the TWIC card by performing biometric identification of the TWIC-holder. We believe the commenter misunderstood the statement in the NPRM, which referred to the use of fake or stolen (but unreported) identification documents, such as drivers licences and birth certificates, to fraudulently obtain an authentic TWIC from the TSA. The use of such fraudulently acquired, but genuine TWICs was one issue highlighted by the GAO and by several commenters as a shortcoming in the TWIC program, and we acknowledge that the use of electronic TWIC inspection will not address that particular scenario. However, we agree with the commenter that if a valid TWIC was stolen after it was produced, electronic TWIC inspection would help to identify such a card if an unauthorized person attempted to use it. Although visual TWIC inspection could also detect such unauthorized use, electronic TWIC inspection would do so more effectively by using the TWIC's biometric and other security features.

Some commenters argued that visual TWIC inspection does not provide ''adequate security,'' and that electronic TWIC inspection should be the standard procedure for all TWIC inspections, rather than used only for high-risk vessels and facilities. The commenter made several arguments as to why visual TWIC inspection should not be used. The commenter quoted guidance from the National Institute of Standards and Technology (NIST), issued with regard to identification for Federal employees when entering Federal facilities, which stated that visual inspection of an identification card offers little to no assurance that the claimed identity of the individual matches the identification. The commenter stated that visual inspection is a weak authentication mechanism and does not provide the level of assurance that an electronic inspection can provide. Another commenter cited the 2011 GAO report on the TWIC program, which stated that visual TWIC inspection was not a particularly effective means of identity verification.[24] While we agree that electronic TWIC inspection provides a more reliable means of identity verification than visual TWIC inspection, we disagree with the assertion that the visual inspection provides no security benefit. Many industries rely on photographic identification cards to verify a card-holder's identity before granting access to accounts or locations. Some situations may require, and justify the cost of, additional layers of security. For example, the heightened risk at Risk Group A vessels and facilities warrant the greater security afforded by electronic TWIC inspection, along with the attendant costs. As explained in this preamble and the accompanying RA, we do not believe such costs are justified for vessels and facilities outside of Risk Group A at this time.

The commenter made several other arguments relating to visual TWIC inspection. First, the commenter noted that there is no way for visual TWIC inspection to determine if a TWIC has been cancelled. While we agree that visual TWIC inspection will not perform an electronic check against the TSA's list of cancelled TWICs, we disagree with the suggestion that visual inspection has no value in performing the card validity check. Security personnel perform the basic card validity check to ensure that a TWIC has not expired by checking the card's expiration date. A TWIC reader does the same validity check electronically, but will further confirm card validity by finding no match on the list of cancelled TWICs. We explain in the RA that the costs associated with this added layer of security are warranted only for Risk Group A vessels and facilities.

The commenter also stated visual TWIC inspection creates vulnerability because it relies on a ''repetitive human process,'' where the staff may become distracted or less attentive. While we agree generally that electronic TWIC inspection is more reliable than visual TWIC inspection, we disagree with the suggestion that visual TWIC inspection is unreliable. We are requiring TWIC readers for Risk Group A, in part, due to the potentially reduced human error that TWIC readers afford. As explained in the RA, that added benefit does not outweigh the costs associated with requiring TWIC readers outside of Risk Group A at this time.

One commenter stated that the background check does not ensure that facilities are protected from crime. The Coast Guard agrees that crimes can still be committed despite background checks, although we note that MTSA specifically prohibits certain persons with extensive criminal histories from receiving TWICs.[25] However, the purpose of requiring electronic TWIC inspection is not to prevent all crime, but to prevent TSIs at high-risk vessels and maritime facilities. In that regard, we believe that TWIC is a critical part of the layered approach to port security because it establishes a minimum, uniform vetting and threat assessment process for mariners and port workers across the country aimed at preventing a TSI. The existing TWIC Program ensures that workers needing routine, unescorted access to secure areas of facilities and vessels undergo lawful status checks (for non-U.S. citizens) and that they are vetted against a specific list in statute of terrorism associations and criminal convictions.[26] It provides a standard baseline for determining an individual's suitability to enter the secure area of a vessel or facility regulated under the MTSA. We note that the program does not exclude everyone with a criminal record and that most, but not all, of the permanent disqualifying crimes for a TWIC can be waived in extraordinary circumstances.[27] However, there are aggressive procedures to remove a TWIC from any TWIC-holder found to have committed one of these crimes after receiving their TWIC, or to remove a TWIC from a TWIC-holder who is later added to any of the terrorism associated databases.

Multiple commenters suggested that the risk analysis for the NPRM did not adequately address cargo containers and the related cargo container facilities. One commenter suggested that container terminals were the primary focus of the enactment of the MTSA and SAFE Port Act, yet they are not subject to the highest level of TWIC scrutiny. The Coast Guard disagrees that container terminals were the primary focus of the Acts, noting that there was substantial discretion permitted by the statutory language to implement electronic TWIC inspection requirements. We reiterate that with regard to threats carried within cargo

[23] 78 FR 17787.

[24] GAO–11–657, ''Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives''

[25] *See* 46 U.S.C. 70105(c) for the list of disqualifying criminal offenses.

[26] 46 U.S.C. 70105 and 49 CFR 1572.103.

[27] 46 U.S.C. 70105 and 49 CFR part 1515.

containers, electronic TWIC inspection is not particularly effective for threat mitigation since scenarios involving container contents (*e.g.,* weapons, personnel) in an attack in the United States do not require access to the container inside the secure area. The risk analysis evaluated the consequence of an attack on the maritime facilities themselves, deeming it reasonable to confine attack scenarios to the facility because offsite scenarios (*e.g.,* transfer of container contents) are not mitigated by TWIC, but are instead the focus of additional layers of protections in the larger MTSA regulatory regime. Based on the MSRAM calculations relating to the effect of an attack on a cargo container facility, the efficacy of electronic TWIC inspections in disrupting such attacks, and considering the costs of requiring electronic TWIC inspections, we arrived at the conclusion that it would not be the most cost-effective approach to improving public safety to require electronic TWIC inspection at these facilities at this time. We would refer interested parties to the accompanying RA for a detailed discussion of alternative regulatory approaches considered in this rulemaking. Furthermore, we note that under existing guidance, any facility not covered by this final rule may implement electronic TWIC inspection on a voluntary basis for any reason.

One commenter stated that the classification for large general cargo container terminals was counterintuitive, because disruption to any one of these facilities could have significant negative consequences for the nation's economy. We understand the commenter's perspective. However, for this rule, as part of the MSRAM analysis, we evaluated the risk of a TSI that (1) occurs at cargo container facilities and (2) would be less likely to occur through TWIC reader implementation, and for these scenarios, the likelihood of long-term disruptions to the nation's economy is assessed to be minimal.

One commenter suggested that not placing container terminals in Risk Group A, and thus not requiring electronic TWIC inspection, would threaten the supply chain by allowing TWIC-holders, who have subsequently been determined by the TSA to be a security threat to the United States, to have unescorted access to the nation's critical infrastructure with impunity. We disagree that not placing container facilities in Risk Group A is tantamount to exposing those facilities to security threats. We note that the general TWIC requirements located in § 101.515, which prohibit those who do not hold a valid TWIC from receiving unescorted access to a secure area, is still effective for these facilities. Container facilities may voluntarily institute requirements for electronic verification, for example, for business reasons. Furthermore, such facilities are subject to spot checks by the U.S. Coast Guard where such invalidated TWIC-holders could be discovered through the use of portable TWIC readers by Coast Guard personnel.

One commenter suggested that terrorists might use a small facility to transport a weapon, thus bypassing electronic TWIC inspection programs. Pursuant to existing requirements, unescorted access to a secure area of any MTSA-regulated maritime facility requires a TWIC, so all workers seeking unescorted access, not just those at high-risk facilities, are subject to background checks. However, we note that electronic TWIC inspection is not designed to directly protect against smuggling, including the smuggling of terrorist weapons. Electronic TWIC inspection is designed to ensure that unauthorized persons, who have not been provided a TWIC, are not provided unescorted access to high-risk vessels and facilities. Many, if not most, smuggling scenarios do not require adversary access to secure areas for success, and thus the enhanced access control afforded by electronic TWIC inspection does little to reduce the risk for these scenarios.

One commenter added that facilities are poor targets for terrorist attacks and thus, screening workers on those facilities adds little value. We disagree, and note that we have tailored this rule to specifically encompass only those maritime facilities where the dangers of a TSI are heightened, such as those that handle or receive vessels carrying CDC in bulk. We have determined that the facilities in Risk Group A could be attractive targets for terrorist attacks due to the substantial loss of life and environmental effects that could result from a TSI. Furthermore, we tailored the requirements to only require electronic TWIC inspection when such inspection would have a substantial effect on reducing the likelihood of such an attack (the ''TWIC utility'' prong of the risk analysis, described in detail in the NPRM). *See* 78 FR 17791.

2. Risk Analysis Methodology

Multiple commenters expressed concern with the risk analysis for this rulemaking. While we have considered the commenters' concerns, our risk analysis model remains unchanged from that proposed in the NPRM. We believe that the existing risk analysis model, which considered a wide range of targets, attacks, and consequences, remains the most comprehensive and logical means available to implement the electronic TWIC inspection program. In this process, the Coast Guard analyzed 68 distinct types of vessels and facilities using the MSRAM database based on their purposes or operational descriptions. The Coast Guard initially separated this list of vessels and facilities into proposed Risk Groups A, B, and C in the ANPRM and have ultimately used this baseline to inform the classification of Risk Group A vessels and facilities in this final rule. We identify these vessels and facilities as those that can best be protected by electronic TWIC inspection.

The risk analysis methodology used in this rulemaking consists of three distinct analytical factors. The first factor, which we described in the NPRM as the ''maximum consequences to [a] vessel or facility resulting from a terrorist attack,'' is the direct consequence of a type of attack that could be prevented or mitigated by use of electronic TWIC inspection. This factor was assessed for each class of vessel and facility. The second factor, which we described as the ''criticality to the nation's health, economy, and national security,'' considered the impact of the loss of a vessel or facility beyond the direct consequences, taking into consideration regional or national impact on health and security. Finally, we considered TWIC utility, which we describe as the effectiveness of the TWIC program in reducing a vessel or facility's vulnerability to a terrorist attack.''

It is important to note that the electronic TWIC inspection program is not the only security measure protecting vessels and maritime facilities, and is not designed to counter every conceivable threat to them. In the preliminary RA, we explained that there were three specific attack scenarios most likely to be mitigated by electronic TWIC inspection, and thus used in our analysis. These scenarios were: (1) A truck bomb, (2) a terrorist assault team, and (3) an explosive attack carried out by a passenger or passerby (with the specific caveat that the terrorist is not an ''insider'').[28] While several commenters criticized certain aspects of the TWIC program for not countering additional threats, we note that benefits outside the scope of the above threats were not considered to be likely successes of the TWIC program and were not considered in our analysis. One commenter suggested that the truck bomb scenario was unrealistic, as it would be easier to

[28] Preliminary RA, p.72.

place a bomb in a container itself. We note that these are two distinct scenarios, and that the risk identified in the latter scenario is one that is not mitigated by electronic TWIC inspection.

The first factor of the analysis was the most comprehensive, which was to determine the direct primary and secondary consequences of the total loss of a vessel or facility. To conduct this stage of the analysis, we used MSRAM data. MSRAM collects data from a wide variety of vessels and facilities and includes calculations of damages for each individual vessel or facility. The damages incorporated into the MSRAM analysis include: (1) Death and serious injuries; (2) direct property damage and the costs of business interruptions; (3) environmental consequences; (4) national security consequences; and (5) secondary economic consequences, such as damage done to the supply chain.[29] To finish the first stage of analysis, we aggregated the MSRAM data from the individual vessels and facilities into averages for each of the 68 identified classes.

The second factor in the analysis considered the impact of the total loss of the vessel or facility beyond the immediate local consequences. This involved examining the regional and national effects of such a loss on the state of human health, the economy, and national security. The third factor in the analysis focused on the effectiveness of the TWIC program in actually reducing the vessel or facility class' vulnerability to a terrorist attack. In instances where electronic TWIC inspection would substantially reduce the effect or likelihood of an attack, this factor was assigned a greater value.

Once the three analytical factors were determined, the Coast Guard combined the scores using the Analytic Hierarchy Process (AHP), developing a total score that combined the severity of an attack and the effectiveness of the TWIC program in countering that attack for each of the classes of vessels and facilities. These overall rankings were then used to determine the Risk Groups used in developing this rulemaking. We believe that this approach used in this risk analysis methodology is highly effective, and represents the best method available for assessing the benefits of the electronic TWIC inspection program to the specific vessels and facilities under consideration.

One commenter suggested that the Coast Guard should not finalize this rule, and that a panel of private industry representatives should be included in an objective review of where the risks and vulnerabilities are in order to develop the best tool for mitigation. The Coast Guard has taken a collaborative approach toward developing this final rule, and has considered information from numerous stakeholders in this rulemaking, including the large number of comments on both the ANPRM and NPRM. As a result, the Coast Guard has amended this final rule, targeting the affected population to those vessels for which the use of electronic TWIC inspection provides the greatest benefit at minimum cost. This would not have been possible without the extensive public input received.

One commenter suggested that previous risk assessments of their operation had never identified a scenario in which rogue employees played a role. We do not agree with the commenter that this weakens the case for the implementation of electronic TWIC inspection requirements. We note that ''rogue employees'' (no precise definition of this term was supplied, but we assume it means an employee who intends to carry out a TSI) are unlikely to be a threat mitigated by this final rule. This final rule is primarily designed to identify and intercept those adversaries who are not employees, but are attempting to use a stolen or otherwise invalid card to gain access to a secure area. A ''rogue employee'' with a valid TWIC would not be intercepted by electronic TWIC inspection. The ''rogue employee'' scenario is partially addressed by the security threat assessment that each employee must undergo before obtaining a TWIC, and is also addressed by other layers of security. For example, 33 CFR 104.285 and 105.275 require owners and operators to have the capability to continuously monitor their vessels and facilities through the use of lighting, security guards, waterborne patrols, automatic intrusion devices, or surveillance equipment.

The same commenter asserted that there are no facts, objective risk assessments, or examples provided to support how a TWIC reader would enhance security absent a known risk or vulnerability. Additionally, the commenter broadly suggested that an owner or operator should be allowed to self-assess and determine its own risk group category after taking into account the security measures already in place at their own location. We disagree with both comments. MSRAM is a fact-based, objective tool for assessing TSI risk in the maritime domain. MSRAM incorporates specific examples of vessels and facility types and various attack modes. As explained in great detail in the ANPRM, NPRM, and elsewhere in this preamble, MSRAM is an analysis tool designed to estimate risk for potential terrorist targets. We consider MSRAM to be the best available tool for determining which vessels and facilities should be considered high-risk for the purpose of TWIC reader requirements. Because electronic TWIC inspection is generally more reliable than visual TWIC inspection, TWIC readers enhance access control more than visual inspection, increasing the likelihood of identifying an aggressor and denying access to secure areas. While the above rationale applies generally to Risk Group A, the Coast Guard also recognizes that the nature or operating conditions of certain vessels and facilities may warrant a waiver from certain regulatory requirements. The existing regulations in 33 CFR 104.130 and 105.130 provide that owners and operators may apply for a waiver of any requirement of the security regulations in 33 CFR parts 104 and 105 (including the TWIC reader requirements) in appropriate circumstances and where the waiver will not reduce overall security.

Several commenters noted that while the Coast Guard used the MSRAM data to conduct its risk analysis, a number of TWIC Pilot Program participants were not contacted during this assessment. They argued that these participants could have provided local knowledge to produce supportable conclusions relative to risks and risk mitigation strategies in particular locations. We believe that these commenters misunderstand how MSRAM data were used. The Coast Guard carefully reviewed the pilot project in writing this final rule. MSRAM datawere used to help determine the consequences of a TSI. This was one factor used in determining the overall risk to the various classes of facilities analyzed in the Coast Guard's risk analysis. The Coast Guard uses MSRAM in a variety of risk analysis applications and does not engage in discussion with each participant every time the data are utilized.

Some commenters also argued that they were the subject of several counterterrorism studies, and that these studies had not identified TWIC as risk mitigation tool, nor had they identified a scenario in which an employee bringing harm to a ferry was an identified vulnerability. These studies were not provided by the commenter but, from their descriptions, seem to have focused on risks other than those posed by persons impersonating

[29] Preliminary RA, p.75.

employees. We note that while previous studies may not have identified TWIC as a risk mitigation tool, we have considered various scenarios in which electronic TWIC inspection would mitigate risk, and used them as the basis for our risk analysis. Furthermore, we note that electronic TWIC inspection is not designed to prevent a valid and cleared employee from bringing harm to a vessel or facility. Instead, it is specifically designed to prevent access to a secure area by an unauthorized person who is attempting to gain access by using a stolen or counterfeited TWIC. We believe that electronic TWIC inspection is an appropriate and cost-effective tool to mitigate such risks.

*B. Electronic TWIC Inspection*

Electronic TWIC inspection is the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the stored biometric template. This process consists of three discrete parts: (1) Card authentication, in which the TWIC at issue is identified as an authentic card issued by the TSA; (2) the card validity check, in which the TWIC is compared to the TSA-supplied list of cancelled TWICs [30] to ascertain that it has not been revoked, and is not expired; and (3) identity verification, in which the TWIC is matched to the person presenting identification through use of a biometric template stored on the TWIC.

The purpose of electronic TWIC inspection is to improve the inspection of TWICs, as compared to visual TWIC inspection. We note that visual TWIC inspection accomplishes the same three tasks as electronic TWIC inspection, but in different ways, and generally not as thoroughly or reliably as electronic TWIC inspection. Visual card authentication is accomplished by visually inspecting the security features on the card (such as the watermark). A visual card validity check is accomplished by checking the expiration date on the face of the card, although there is no way to visually check if the TWIC has been revoked by the TSA since it was issued. Finally, visual identity verification is conducted by comparing the photograph on the TWIC with the individual's face.

Electronic TWIC inspection improves upon the visual inspection checks, and adds two additional benefits. In electronic TWIC inspection, the authenticity of the card is verified by issuing a challenge/response to the TWIC's unique electronic identifier, called a Card Holder Unique Identifier (CHUID). The card's validity is determined by checking the TWIC against the most recently updated list of cancelled TWICs. Finally, the identity of the TWIC-holder is verified by matching the biometric template stored on the TWIC to the individual's biometrics. Each of these methods is an improvement upon visual TWIC inspection as the electronic TWIC inspection uses methods of validation that are not easily manipulated through means such as counterfeiting or altering the surface of the TWIC. Additionally, electronic TWIC inspection ensures that the card being presented has not been invalidated by a means other than being expired, such as the card having been reported lost, or the TWIC being revoked due to a criminal conviction.

TWIC inspection, either electronic or visual, provides a baseline of information to determine who may be provided unescorted access to secure areas of MTSA-regulated vessels and facilities. While not every TWIC-holder is authorized unescorted access, the TWIC ensures that facility security personnel do not grant unescorted access to individuals that have not been vetted or have been adjudicated unfit for access to secure areas.

Several commenters suggested that the sole purpose of TWIC is for a worker to be vetted through security and criminal checks, and that access control is not a purpose of the TWIC program. We disagree with this description of a fundamental principle of the TWIC program. The controlling statute, 46 U.S.C. 70105(a)(1) reads, in part, ''[t]he Secretary shall prescribe regulations to prevent an individual from entering an area of a vessel or facility that is designated as a secure area . . . unless the individual holds a transportation security card issued under this section. . .''. This is a clear mandate for an access control program. We have implemented this mandate by requiring maritime workers to obtain a TWIC, and by requiring owners and operators to inspect each individual's TWIC prior to granting access to secure areas. Using the biometric template, TWIC provides a highly secure means for security personnel to verify the identity of an individual seeking access to a secure vessel or facility and implementing this core requirement of the MTSA.

In this final rule, we are revising the regulatory text to add flexibility and more accurately reflect the electronic TWIC inspection process. In the NPRM, we did not describe the process as ''electronic TWIC inspection,'' but stated in proposed § 101.520(a) that ''all persons must present their TWICs for inspection using a TWIC reader, with or without a . . . PACS. . .''. [31] In this final rule, we are modifying the process from presentation of a TWIC to a TWIC reader to the concept of electronic TWIC inspection. As stated below, and as defined in section 101.105 of this final rule, ''Electronic TWIC inspection'' means the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the stored biometric template. In doing so, we have laid out the exact requirements for this process in revised § 101.520.

In this section, we address the comments and concerns submitted in response to the NPRM, and describe in detail how electronic TWIC inspection will work in a wide variety of operational situations. Table 2 provides a summary of the acceptable implementation options for owners and operators to perform electronic TWIC inspection. The owner or operator of a vessel or facility must ensure the options chosen to meet the electronic TWIC inspection requirements perform the required card authentication, card validity, and identity verification required in revised § 101.520.

[30] We note that at this time, this list is the Cancelled Card List (CCL). However, there are also several specific Certificate Revocation Lists maintained by TSA, which differ from the CCL. In order to provide a regulation that is flexible in terms of future technology adaptations, in this final rule, we have described the list in the regulatory requirement generically as the ''list of cancelled TWICs.'' *See* sections 101.520(b) and 101.525 of the final rule regulatory text. This allows TSA to continue to use the CCL, but will also allow additions from various Certificate Revocation Lists if and when that becomes feasible and efficient. Any such change in the list of cancelled TWICs would be a ''back end'' change on TSA's part and would not impact the burdens or operations of private parties, who would still only be required to check a TWIC against the list as part of the card validity check. In this document, we generally refer to the ''list of cancelled TWICs'' when referring to the regulatory requirements in the final rule, while still using the ''CCL'' terminology when discussing comments on the Cancelled Card List or discussions in the NPRM that used that terminology.

[31] 78 FR 17829.

TABLE 2—IMPLEMENTATION OPTIONS

| Option | Description |
|---|---|
| TWIC Reader (QTL) ..... | Owner/operator uses a TWIC reader listed on TSA's QTL. To gain entry to a secure area, employee presents TWIC and biometric for electronic inspection. |
| TWIC Reader (non-QTL) ..... | Owner/operator uses a TWIC reader that adequately performs the three required electronic checks (card authentication, card validity check, identity verification). To gain entry to a secure area, employee presents TWIC and biometric for electronic inspection. |
| Transparent Reader ..... | Similar to non-QTL TWIC reader, except the Transparent Reader does not independently perform card validation, card authentication, and identity verification. Instead, the Transparent Reader transmits information from the employee's TWIC and biometric to a back end system containing software that performs the TWIC check. Once the TWIC check is complete, the back end system shall perform what processes are required to either grant or deny access. |
| PACS (with facility access card). | Employee is issued a facility access card after initially registering employee's TWIC and biometric into the facility's access control database. To gain entry to a secure area, employee presents facility access card and biometric for electronic inspection to match against employee's record in the facility's database. |
| PACS (with biometric only) .. | Employee's TWIC and biometric are initially registered into the facility's access control database. To gain entry to a secure area, employee presents biometric (e.g., fingerprint) for electronic inspection to match against employee's record in the facility's database. |

1. Electronic TWIC Inspection Does Not Necessarily Require a TWIC Reader

Many commenters expressed concerns regarding the costs of purchasing, installing, and using TWIC readers that have been approved by the TSA. They argued that the costs of the TWIC readers were high, and that there were problems with the reliability of TWIC readers and cards. Many commenters requested that the Coast Guard extend guidance issued in Navigation and Vessel Inspection Circular (NVIC) 03–07 and Policy Advisory Council (PAC) Decision 08–09, change 1, in which we outlined how an existing PACS could be used in lieu of a TWIC reader until the TWIC final rule was issued.

In NVIC 03–07, we described how TWIC could be incorporated into an access control system even if the person accessing the secure area did not physically use the TWIC as an access control card. We stated that:

*Example:* A facility employee who possesses a valid TWIC is registered into the facility's access control database and is issued a facility access card after the TWIC is verified visually as described in 3.3 a. (7) [of NVIC 03–07]. To gain entry into a secure area, the employee inserts or scans his/her facility access card at a card reader, which verifies the access card as a valid card for the facility. The TWIC does not need to be used as a visual identity badge at each entry once the facility-specific card is issued. The card reader then verifies the individual by matching the facility access card to the individual's record in the facility database and allows access to secure areas as dictated by the permissions established by the owner/operator in the access control system. By virtue of the fact that the employee would not be issued a vessel or facility-specific card without first having a TWIC, the requirement to possess a TWIC for unescorted access to secure areas is met.[32]

Many commenters noted, and we are aware that, the proposed regulatory text in the NPRM was worded in such a way that rendered this method of compliance impossible. The proposed regulatory text in § 101.520(a)(1) stated ''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.'' [33] Similarly, proposed §§ 101.525 and 101.530 required visual inspections of TWICs before permitting access. Many commenters took issue with the change in approach from current requirements as described in the NVIC.

In this final rule, we are revising the regulatory text to allow electronic TWIC inspection to be conducted by either a TWIC reader or a PACS at vessels and facilities. This regulatory language will supersede previous guidance documents such as PAC 08–09, change 1 and NVIC 03–07. Under the new language in revised section 101.520 we are providing greater flexibility on the type of equipment used, as long as the three parts of electronic TWIC inspection are performed satisfactorily.

Multiple commenters discussed the scenario where an owner or operator has a PACS which cross-checks successful electronic TWIC inspections against employment records and other internal security systems and records to verify that the cardholder works for the company, holds current certifications, and should be allowed into the facility. As explained in this document in Section V.B., such a system could meet the requirements for electronic TWIC inspection as revised for this final rule.

Two commenters at a public meeting suggested that if a facility could prove its PACS is superior to the TWIC requirements, then the facility should be exempt from them. Similarly, other commenters suggested alternatives the Coast Guard could require, including a color-coded system analogous to the former Homeland Security Advisory System. In this final rule, we are not providing a generalized exemption from electronic TWIC inspection requirements as suggested by the commenters. However, as explained, such requirements can be performed by a PACS, thus potentially eliminating the need for these particular commenters to purchase entirely new equipment or the need for an exemption from the electronic TWIC inspection requirements.

Multiple commenters stated that it would be more cost effective in some cases to purchase one or two stationary TWIC readers, but also to purchase several portable TWIC readers for multiple temporary gates or entrances. One commenter asked whether the final rule requires fixed card readers at every point of access, even a temporary or infrequently used one. The same commenter asked whether portable TWIC readers would meet the TWIC reader requirements on an OCS facility. We clarify that neither the NPRM nor final rule required stationary TWIC readers. The final rule, as described above, allows for flexibility in terms of equipment.

The arrangements the commenters suggested could all be accommodated by this final rule. In this final rule, we are removing prescriptive requirements regarding the permanence, type, and placement of electronic readers. If a

[32] Enclosure (3) to NVIC 03–07, p. 1515 (Available in the docket by following the instructions in the **ADDRESSES** section of this preamble).

[33] 78 FR 17829.

vessel or facility has an existing access control system, of any variety, whose electronic readers perform the requirements of the electronic TWIC inspection (including identity verification), and are approved under the relevant security plan, then the PACS is permissible.

In response to the many comments we received on this issue, in this final rule, we are substantially altering the TWIC reader requirements to accomplish the goals set out by the TWIC reader program, but in a manner that provides more flexibility in terms of how those goals are met. The requirements in this final rule are designed to allow as much flexibility in design of an access control system as possible while still achieving the goals of the TWIC reader program.

We believe that the increased flexibility offered by the revised, performance-based regulations is responsive to the many commenters who described existing access control systems that they believe are better suited for their individual vessels and facilities than those proposed in the NPRM. Under these final regulations, a system that accomplishes the goals of the TWIC program and uses the three electronic checks mandated by the regulation will be considered by the Coast Guard when reviewing the security plans. As long as the Coast Guard agrees that the proposed security plan accomplishes the goals in a robust fashion, we will not limit the choices of the means to do so.

2. Integrating Electronic TWIC Inspection Into a PACS

NVIC 03–07 and PAC 08–09 change 1 explain that they are valid guidance until a TWIC reader final rule is issued, but many commenters requested that these documents remain valid even after the final rule becomes effective. Because this final rule significantly changes the TWIC inspection process for Risk Group A vessels and facilities, the TWIC-specific guidance provided in those documents will not continue to apply to Risk Group A. However, because we are not making any changes to the TWIC requirements for those vessels and facilities not in Risk Group A, the guidance documents still retain their validity with regard to those entities. We will update and post these guidance documents online at *https://homeport.uscg.mil/* prior to the effective date of this final rule.

In this final rule, we no longer require facility and vessel operators to use a TWIC reader listed on the QTL each time a person is granted unescorted access to a secure area. Instead, we are permitting multiple options as previously described, including the use of a PACS approved in the required Facility Security Plan (FSP) or Vessel Security Plan (VSP), if the PACS can perform the electronic TWIC inspection requirements.

*Example:* A facility employee who possesses a valid TWIC is registered into the facility's access control database and is issued a facility access card after the TWIC is verified in accordance with 33 CFR 101.530. After the TWIC and holder of the TWIC are validated to ensure the TWIC is issued by TSA and the holder of the TWIC is bound to the TWIC, a biometric template of the employee is taken and stored on the facility access control system. To gain entry into a secure area, the employee inserts or scans his or her facility access card at a card reader, which verifies the access card as a valid card for the facility. The card reader then matches the facility access card to the employee's record in the facility database. A biometric sample from the employee is taken and matched to the associated biometric template stored on the facility's access control system. The facility's access control system then checks the TWIC's CHUID to assure that the TWIC is still valid (unexpired) as well as checks the list of cancelled TWICs to ensure that it has not been cancelled for any other reason. Upon verification that the TWIC is valid and the employee's biometric matches the associated template, the facility access control system allows access to secure areas as dictated by the permissions established by the owner or operator in the access control system. By virtue of the fact that the employee would not be issued a facility-specific card without first having a TWIC, the requirement to possess a TWIC for unescorted access to secure areas is met. The requirement for a biometric match of the employee is met through the performance of a match to the biometric template stored on the facility access control system.

We note that the requirement for electronic TWIC inspection can be met even without the use of any sort of card reader, so long as the three parts of the electronic TWIC inspection are met. Such a system could be designed to use an individual's biometric check as a means of identification, such as described below.

*Example:* A facility employee who possesses a valid TWIC is registered into the facility's access control database and a biometric template of the employee is taken and stored on the facility access system. (We note that this is done after the TWIC and holder of the TWIC are validated to ensure the TWIC is issued by TSA and the holder of the TWIC is bound to the TWIC). To gain entry into a secure area, the employee presents a biometric (*e.g.*, fingerprint) to a biometric reader connected to the facility's access control system. The access control system identifies the employee from the fingerprint and then matches it to the biometric template and the employee's TWIC information in the facility database. The facility's access control system then checks the TWIC's CHUID to assure that the TWIC is still valid (unexpired) as well as checks the list of cancelled TWICs to ensure that it has not been revoked for any other reason. Upon verification that that the TWIC is valid and the employee's biometric matches the associated template, the facility access control system allows access to secure areas as dictated by the permissions established by the owner or operator in the access control system. By virtue of the fact that the employee would not be entered into the facility's access control system without first having an authenticated TWIC, the requirement to possess a TWIC for unescorted access to secure areas is met. The requirement for a biometric match of the employee is met through the performance of a match to the biometric template, in this case a fingerprint stored on the facility access control system.

Additionally, we note that although a biometric template is the particular biometric measurement used in the TWIC application process, an alternative biometric may be used to perform the identity verification check required by the regulations so long as the method is approved in the security plan. For example, as two commenters suggested, a vascular scan could be stored on a facility's access control system instead of a fingerprint, which could be useful in situations where some employees have difficult-to-read fingerprints.

a. List of Acceptable TWIC Readers

In the NPRM, the Coast Guard proposed that only certain TWIC readers would be permitted to be used for purposes of electronic TWIC inspection. As stated above, proposed § 101.520(a)(1) read, ''[p]rior to each entry, all persons must present their TWICs for inspection using a TWIC reader, . . .''. The term ''TWIC reader'' was defined in proposed § 101.105 as ''an electronic device listed on TSA's Qualified Technology List . . .''. Thus, by operation of the proposed regulatory text, TWIC readers listed on the QTL would be required at access points to secure areas on facilities and at the entrances to vessels requiring electronic TWIC inspection.

TSA had not published the QTL at the time of publication of the NPRM. Thus, in its discussion regarding the types of approved TWIC readers, the NPRM reiterated guidance from PAC–D 01–11 regarding the use of TWIC readers to meet the existing regulatory requirements for effective identity verification, card validity, and card authentication.[34] Specifically, in that guidance document, we stated that:

In accordance with 33 CFR 101.130, the Coast Guard determines that a biometric

[34] 78 FR 17805.

match using a TWIC reader from the TSA list of readers that have passed the Initial Capability Evaluation (ICE) Test (available at: *http://www.tsa.gov/assets/pdf/twic_ice_list.pdf*) to confirm that the biometric template stored on the TWIC matches the fingerprint of the individual presenting the TWIC meets or exceeds the effectiveness of the identity verification check.

The NPRM also noted that, in accordance with the guidance, ''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 of TWIC readers.'' [35]

In recognition of advancing technology and standards, and to provide further flexibility to the end user that may meet business specific needs, this final rule does not require a TWIC reader from the TSA's QTL, accessible online at *http://www.tsa.gov/stakeholders/reader-qualified-technology-list-qtl.* Instead, the Coast Guard is permitting multiple options for the implementation of electronic TWIC inspection. The first option for meeting these needs within this final rule remains the mechanism proposed in the NPRM, which is the use of TWIC readers listed on the QTL. These TWIC readers are defined as ''Qualified Readers.'' We believe that this option is most appropriate for vessels or facilities that currently do not conduct electronic TWIC inspection and are seeking a TWIC reader determined to be in conformance with the TWIC Reader Hardware and Card Application Specification, available in the online docket for this rulemaking. The QTL continues to remain useful for this and other purposes.

A similar option would be to use a TWIC reader that is not on the QTL. While such electronic readers are not prohibited by this rule, they must still meet the performance requirements of § 101.520. This performance-oriented option is intended to provide more options to users to meet their individual needs while still relying on the TWIC as an access control credential.

Another option would be to use an electronic reader or combination of separate devices—such as proximity readers, biometric readers, and PIN pads—that would transmit the information from the TWIC and individual seeking access to software that performs the card authentication, card validity check, and biometric identification functions required in § 101.520. We refer to this arrangement as a ''Transparent Reader.'' In this case, for example, a Transparent Reader would read the information from the TWIC along with the biometric sample provided by the individual and transmit it to a back end system containing software that performs the TWIC check. Once the TWIC check is complete, the back end system would perform what processes are required to either grant or deny access. This option may be highly popular with facilities that have already invested in electronic reader infrastructure and high tech software systems that may not be on the QTL. In this case, much as a situation with a PACS, the operator may have to add a biometric component, if not already in place, and modify software to include TWIC compatibility, but would not have to replace the entire system.

The last option, described in detail above, would be the use of an existing PACS, with the inclusion of biometrics, with a facility-specific access card that uses the TWIC as the baseline credential. This is purely a performance requirement, and would not require the use of government-approved equipment. In this case, the PACS would be required to match the TWIC against the list of cancelled TWICs and, if positively matched, automatically cancel the facility access card so as to not allow unescorted access to secure areas of the facility.

Several commenters provided comments that addressed the specific types of approved card readers, but we believe that many of the concerns raised by commenters are resolved by the Coast Guard moving to a more flexible series of options for conducting electronic TWIC inspection. One commenter in a public meeting expressed concern that there was not an approved card reader which he could use for cost estimates. We note that the TSA now has a list of approved TWIC readers, which is available on the Coast Guard's Homeport site.[36] One commenter suggested that this rule was not in alignment with the TSA's Request for Information regarding development of the QTL. We disagree, and note that the Coast Guard and TSA worked closely in developing and implementing the electronic TWIC inspection requirements. Furthermore, we note that with the additional flexibility afforded by this final rule, equipment to conduct electronic TWIC inspections is available at a wide variety of prices, depending on the manner in which electronic TWIC inspection is conducted. Additional information on cost estimates is provided in the final RA accompanying this final rule.

Additionally, one commenter requested that software be included on the QTL. We note that the list of TWIC readers on the QTL includes TWIC reader and software pairings. Beyond the physical aspects of TWIC reader testing in terms of environmental or drop testing, a large portion of what is tested in the QTL process is the software.

Other commenters suggested that, based on the TWIC Pilot Program, TWIC reader technology is still not ready for requiring TWIC readers at facilities, and requested that this final rule be delayed. Similarly, one commenter recommended that the Coast Guard only proceed with the rule if it was confident in the reliability of existing TWIC readers. We believe that not only has technology continued to improve, but also additional flexibility has been afforded in this final rule, both of which should alleviate problems with specific TWIC readers used in the pilot. Vessels and facilities required to conduct electronic TWIC inspection can choose from a wide variety of means so as to meet their budget and operational needs. Furthermore, the flexibility built into this final rule allows for future advancement of both card and reader technologies in a manner that will provide for further reductions in impact on business operations of the maritime industry.

b. PIN Pads and Biometric Input Methods

One issue raised in the ANPRM was the use of PINs as part of the identification process. We note that upon getting a TWIC, each TWIC-holder is required to remember a PIN. As proposed in the NPRM, under most circumstances, the TWIC-holder would not be required to provide the PIN when seeking access to secure areas, except as a backup measure when the TWIC-holder's biometric template is unreadable. For this reason, there is no requirement that access control systems have the capability to accept a PIN.

Comments relating to the use of PINs were generally negative. Several commenters specifically argued against the use of PINs. Some commenters stated that because the PINs are rarely used, they are seldom remembered by TWIC-holders. We agree that rarely-used PINs will likely be forgotten, and thus the only people who would likely remember their PINs are those who use them regularly, such as those with impaired biometrics. Similarly, one commenter stated that 100 percent of cardholders would need to visit one of

[35] 78 FR 17805.

[36] We have also included the current version of the list in the docket USCG–2007–28915.

the TWIC enrollment centers to reset or establish a new PIN in the event that the Coast Guard required PIN entry, implying that without regular use of PINs, they are quickly forgotten.

PINs would not be required or permitted as a substitute for biometric identification of most users. Instead, this rule provides that PINs are available as an alternative only for individuals whose biometrics can not be read. The Coast Guard recognizes that for some people, taking a biometric read can be problematic. For example, people with severely injured fingers are often unable to have their fingerprints read. For such cases, the final rule provides an alternative means to ensure identity verification. As stated in § 101.520(c)(2), the use of a PIN plus a visual TWIC inspection is an acceptable alternative to a biometric match for individuals who are unable to have their biometric template captured at enrollment or who have unreadable biometrics due to injury after enrollment. For that reason, owners and operators may find it expedient to include an electronic reader with a PIN pad in at least some of their access control locations to accommodate people with unreadable biometrics.

3. Comments Related to Troubleshooting TWIC

This section elaborates on certain programmatic issues relating to electronic TWIC inspection, specifically, how to address problems arising if either the electronic reader or access card malfunctions. In this section, we elaborate and expand on the provisions described in the NPRM as well as address issues raised by commenters.

In the NPRM, the Coast Guard proposed regulations in § 101.535 that laid out requirements for TWIC inspection in special circumstances where a malfunction in the TWIC inspection system has occurred. In paragraph (a), we described how access could be granted in the event of a lost, stolen, or damaged TWIC card. In paragraph (b), we proposed how access could be granted in the event that a person's biometric template could not be read due to either technology malfunction or the inability of an individual to provide a biometric template. In paragraph (c), we proposed that in the event of a TWIC reader malfunction, an individual could still be granted unescorted access to secure areas for a period not to exceed 7 days, provided that individual has been granted such unescorted access in the past and is known to possess a TWIC. We note that the period in paragraph (c) was extended to 37 days in CG–FAC Policy Letter 12–04.

Because the final rule, as written, sets forth a requirement for electronic TWIC inspection rather than specifically requiring that a TWIC be read by a TWIC reader, the text of this section needs some alterations to account for the new flexibility. We have integrated these alterations into the final regulatory text as detailed in the sections below. Furthermore, we have considered the requests and arguments of various commenters, and we are integrating many of the ideas presented into the final rule. Finally, we have attempted to modify and clarify the regulations where appropriate.

a. Lost, Stolen, or Damaged TWIC

The NPRM proposed that if an individual cannot present a TWIC because it has been lost, damaged, or stolen, the individual could be granted unescorted access for a period of up to seven days if various conditions were met. The conditions include the individual previously having been granted unescorted access, being known to have had a TWIC, being able to present alternative identification, and having reported the TWIC as lost, stolen, or damaged to the TSA. This proposed language was derived from existing requirements in 33 CFR parts 104 through 106. Additionally, in CG–FAC Policy Letter 12–04, the Coast Guard allowed an individual to be granted unescorted access for an additional 30 days (for a total of 37 days of unescorted access), if the individual provided proof that a replacement TWIC had been ordered. Policy Letter 12–04 also allowed unescorted access to those individuals with expired TWICs who had applied for a TWIC renewal prior to expiration.

i. Vessels and Facilities Using a PACS

Because the final rule provides more flexibility for electronic TWIC inspection beyond presenting a TWIC for access control purposes, some of the issues addressed in § 101.535 are significantly different if using a PACS to perform the electronic TWIC inspection. For example, if an employee's TWIC is stolen and the theft is reported to the TSA, the affected TWIC will be placed on the list of cancelled TWICs, but the employee will still be registered in the facility's PACS. However, upon attempting to gain access to a secure area, during the card validity check, the affected TWIC will appear on the list of cancelled TWICs, and thus fail the check. The revised final regulations are designed to allow a procedure where the employee can still be granted unescorted access until he or she can obtain a replacement TWIC and update his or her profile in the facility access control system with the information from the new TWIC. In this final rule, we have added § 101.550(b), which allows unescorted access to secure areas to be granted by a facility operator for a period of up to 30 days if the TWIC appears on the list of cancelled TWICs if the individual is known to have had a TWIC and to have reported it lost, damaged, or stolen.

*Example:* An individual who works at a facility where the PACS has been linked to a TWIC card reports his or her TWIC as lost. When presenting his or her facility access card to the PACS, the card validity check will return a TWIC on the list of cancelled TWICs because the TWIC has been reported lost. The FSO confirms that the TWIC was reported as lost. In that instance, the PACS will recognize the status of the TWIC as cancelled, but can still grant unescorted access to secure areas to the individual for a period of up to 30 days. If, after 30 days, the individual has not linked their facility access card to a valid TWIC, the PACS would have to deny unescorted access to secure areas to that individual.

ii. Vessels and Facilities Using TWIC Readers

We proposed in § 101.535 that vessel or facility operators using TWIC readers allow for temporary access in the case of a lost, stolen, or damaged TWIC. Specifically, the Coast Guard proposed that if a person is known to have had a TWIC, has previously been granted unescorted access, and can present another form of acceptable identification, and there are no other suspicious circumstances, then the operator may grant that person access for 30 days so that they can be issued a new TWIC.

We received a wide variety of comments relating to the issue of lost or stolen TWICs. One commenter argued that any allowance for malfunctioning TWICs undermines the point of having the card at all. We disagree, and note that the procedure is necessary to ensure smooth operation of the TWIC system, and believe it contains enough safeguards so as not to function as a loophole in security.

One commenter recommended splitting the CCL into separate categories, including categories of TWICs invalidated for ''administrative reasons.'' We disagree, because the list of cancelled TWICs is intended to help screen out invalid cards regardless of the reason.

Many commenters argued that the 7-day period proposed in § 101.535(a) is too short, and that the period should be extended, with a significant number of

these commenters referring to the 30-day extension of the 7-day period permitted by CG–FAC Policy Letter 12–04. Based upon the comments received, which indicated that it can take longer than 7 days to be issued a new TWIC, we have decided to include a 30-day period for this situation in section 101.550(b) of the final rule. We believe that this provides ample time to be issued a new TWIC, without presenting an undue security risk. When effective, this regulation will supersede the current guidance in CG–FAC Policy Letter 12–04, which allowed for a total of 37 days.

b. Transportation Worker Forgets To Bring TWIC To Work Site

The existing regulations in 33 CFR parts 104 through 106, the policy arrangements in CG–FAC Policy Letter 12–04, as well as the proposed regulations in § 101.535, only grant unescorted access to those individuals whose TWICs have expired or have reported their TWIC as lost, stolen, or damaged to the TSA. For all other individuals who fail to present a TWIC, unescorted access would be denied under proposed § 101.535(d). Thus, under the proposed regulation, an employee who forgot his or her TWIC at home would not be permitted unescorted access to the facility, whereas an employee whose TWIC was stolen would be permitted unescorted access for a limited period of time.

We received one comment relating to the issue of forgotten TWICs from a commenter who described such a situation in their submission to the docket for this rulemaking. This commenter suggested that we add an allowance for persons who forgot their TWIC at home. After reviewing comments on the proposed rule, we reiterate our existing position that persons who cannot present a valid TWIC, and have not reported their TWIC as lost, stolen, or damaged to the TSA, may not be granted unescorted access to a vessel or facility.

We believe that providing an exemption for forgotten TWICs creates a potential degradation in security and additional risks that outweigh the benefits. Unlike the situation where a TWIC has been reported as stolen or lost to the TSA and is therefore no longer valid which can be verified by checking the list of cancelled TWICs, a claim of a forgotten TWIC cannot be validated.

Instead, we reiterate that under current regulation at § 101.514(a), unless exempted from the TWIC requirements by § 101.514(b), (c), or (d), all persons must physically possess a TWIC, or undergo electronic TWIC inspection, prior to being granted unescorted access to a secure area of a vessel or facility. Persons who do not physically present a TWIC or undergo electronic TWIC inspection, and have not reported their TWIC as lost, stolen, or damaged to the TSA, may not be granted unescorted access.

c. Inaccessible Biometrics

In the NPRM, we proposed two secondary authentication procedures that could be followed in the event that a person's biometric template could not be read by a TWIC reader or PACS due to a technology malfunction or low quality biometric template. These alternatives were listed in proposed § 101.535(b), and allowed either the input of a PIN or the use of an alternative biometric that has been incorporated into the PACS. Given the change from requiring a TWIC reader to requiring electronic TWIC inspection, some changes to this section are needed as well. We discuss changes to this section and comments received below.

One commenter suggested that people with unreadable biometric templates should be allowed to use a PACS card in addition to a PIN or alternate biometric. We agree, and note that under the final regulations, given that input of biometric information (including alternatives to fingerprints) into a PACS reader may now be a common manner of completing identification verification, the use of a PACS card in conjunction with an alternative biometric will be an accepted regular way to conduct an electronic TWIC inspection.

However, upon consideration, we do not believe that the input of a PIN alone is equivalent to biometric identification. Biometric identification allows the facility to ascertain with a high degree of certainty whether the individual requesting access is the TWIC-holder. On the other hand, commenters noted that other methods of identification verification will not detect counterfeit, stolen, or borrowed TWICs. Similarly, the use of a PIN alone will not detect a borrowed TWIC or PACS card or, potentially, a stolen TWIC or PACS card, if the PIN has been illicitly obtained.

Nonetheless, the Coast Guard believes that a method for accommodating persons with unreadable biometrics is important. In such cases, we believe that visual TWIC inspection, when combined with the PIN, provides enough certainty as to be an acceptable alternative to biometric identification. Combining visual identification with the PIN will help to ensure that stolen and borrowed cards are difficult to use.

Thus, in this final rule, we are modifying the provision in proposed § 101.535(b), which allowed for PINs to be used in lieu of biometric matching, to include a requirement for visual identification in addition to the PIN. The new provision is located in § 101.550(c) of this final rule. We believe that this provision would present few problems, as people could use their TWICs for visual identification. Alternatively, if a PACS PIN is assigned and stored in the access control system, an employee with unreadable biometrics could enter his or her PIN and present a PACS card or driver's license to conduct a visual identification check.

d. Malfunctioning Access Control Systems

In the NPRM, we proposed a mechanism by which persons could be granted unescorted access to secure areas if a TWIC reader malfunctioned. Specifically, proposed § 101.535(c) allowed owners and operators to use visual checks for a period of 7 days if a TWIC reader malfunctioned. In light of the change in this final rule from the required use of TWIC readers to the more flexible requirement for electronic TWIC inspection for Risk Group A vessels and facilities, we are making some conforming changes and clarifications to this procedure. We received several comments on the matter, which are addressed below.

Upon consideration of this policy, we believe that a clause automatically allowing the use of visual TWIC inspections in lieu of biometric matching presents a serious security concern. As one commenter argued, any allowance for malfunctioning TWICs undermines the point of having the card at all. The Coast Guard agrees, and believes that allowing the use of visual TWIC inspections in lieu of biometric matching degrades security. This final rule represents a concerted effort to significantly upgrade the security at a relatively small group of high-risk vessels and facilities. Given the importance of security, we would not expect vessels or facilities to have only a single TWIC reader, but expect some redundancy in the system, and note that two commenters strongly echoed the view that redundancy is needed in any critical system. We would agree that, as a practical matter, the minimum number of electronic readers (either dedicated TWIC readers or those integrated into a PACS) at a facility or onboard a vessel would be two, in case one malfunctioned. As discussed in the RA, using the TWIC pilot data we estimated the average number of electronic readers

required by this final rule by facility and vessel types at a minimum 2 per vessel and 4 per facility (Tables 4.3 and 4.4 of the RA). While the TWIC readers on the QTL have been tested to ensure a degree of reliability, there are many factors external to the testing process that could cause any one individual electronic reader to fail. The immediate availability of a backup electronic reader should one fail (as documented in the relevant security plan) would allow a vessel or facility to maintain the appropriate level of security for access control and continue operating without further burden. Due to the security concerns discussed in this paragraph, we are removing from the final rule the proposed provision in § 101.535 that would have permitted automatic transition to visual TWIC inspections in the event of an electronic reader malfunction. As stated above, based on discussions with industry we expect that owners and operators will have an additional functioning electronic reader to use in those instances in case of equipment failures or malfunctions (§§ 104.260(c) and 105.250(c)). If the owners and operators plan for malfunctions as existing regulations require, there should be no significant disruption of operations. Further, in the unlikely event that both primary and redundant electronic readers malfunction, the owner or operator could obtain permission from the Captain of the Port (COTP) to continue operating.

Two commenters suggested changing the language in proposed § 101.535(c) from a ''reader malfunction'' to ''in the event of an access control system failure,'' noting that many other systems (such as the software or electricity) could fail, thus rendering an electronic reader inoperable. As we are deleting this exemption in this final rule, the language question is no longer at issue.

Commenters also suggested that 7 days is not sufficient to correct all problems that can result in a TWIC malfunction. They noted that it might take longer to procure parts, especially after a major regional disaster or holiday, and that a 15-day period where visual TWIC inspection is permitted would be more reasonable. On the other hand, one commenter suggested that it should take only hours to repair a malfunctioning TWIC reader. In this final rule, we are removing this provision. Thus, restoration of an access control system will be handled in accordance with the procedures for the reporting requirements for non-compliance in §§ 104.125, 105.125, and 106.125, which require the owner or operator to notify the cognizant Captain of the Port and either suspend operations or request and receive permission from the COTP to continue operating. Similarly, in the event of a total system collapse or regional disaster, the COTP will work with the affected organization to restore an access control system as expeditiously as possible.

The following examples provide illustrations relating to scenarios involving the failure of an access control system:

*Example:* A facility using TWIC readers at five access points suffers equipment failure of TWIC readers at two of those access points. The facility would still be able to permit unescorted access through the remaining three access points. Unescorted access could also be granted using portable TWIC readers at the two affected access points immediately in accordance with the FSP. The facility would be required to notify the COTP that this equipment failure took place but could continue operations using the remaining TWIC readers.

*Example:* A computer virus causes a facility's PACS to become completely inoperable, but the FSP contains an alternative where access is controlled through the use of portable TWIC readers, compliant with § 101.520, at each access point to secure areas. The facility would be required to notify the COTP that such a failure of the PACS had occurred, but could continue operations uninterrupted by using the portable TWIC readers.

*Example:* A computer virus causes a facility's PACS to become completely inoperable, and the FSP does not contain an alternative means of conducting electronic TWIC inspection. The owner or operator could request permission from the COTP to conduct visual TWIC inspections for a limited time until the PACS is operational. Grants of unescorted access to secure areas would have to be suspended until such permission was granted by the COTP.

Multiple commenters suggested that in the event that a TWIC reader malfunctions, a facility should be immediately able to continue to process workers using an alternative means defined in a security plan, rather than requesting approval from the COTP to do so. One commenter also suggested that an after-the-fact review by the Coast Guard could be used in such circumstances. We note that the proposed text of § 101.535(c) in the NPRM did not propose to require COTP authorization to allow continuing operation for a period of 7 days, so we are unsure of the provision to which the commenter may be referring. Nonetheless, the final regulatory text allows a facility to immediately continue to process workers using an alternative means as defined in an approved security plan as required by §§ 104.260(c) and 105.250(c) without additional COTP approval.

One commenter suggested that the Facility Security Officer (FSO) should be able to determine if there are mitigating circumstances that need to be implemented for a temporary time frame. In such a case, the commenter suggested that the facility would conduct visual identification verification in lieu of electronic TWIC inspection. We disagree with this suggestion, for the reasons described above. The commenter also requested that the COTP be able to waive TWIC requirements in certain circumstances. We note that the COTP has the power to waive requirements or impose alternative equivalent measures generally.

One commenter requested clarification on procedures to be used if TSA's Web site is inaccessible and they are unable to access updates to the CCL. In general, the owner or operator of an access control system is required to download the TSA-supplied list of cancelled TWICs (currently, the CCL) periodically, depending on the MARSEC level, pursuant to § 101.525 of this final rule. However, if the problem with downloading the list is out of the operator's control, such as the TSA Web site being down for an extended period of time, we would consider it acceptable to continue to operate the access control system by using the most recent version of the list available.

e. Requirements for Varying MARSEC Levels

In the NPRM, we proposed requirements for Risk Group A vessels and facilities that would vary based on the MARSEC level. MARSEC levels are set to reflect the prevailing threat environment of the maritime transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States. Specifically, we proposed to require that at MARSEC Level 1, during the card validation process, a TWIC must be checked against a version of the list of cancelled TWICs that is no more than 7 days old. However, at higher MARSEC levels, we proposed that the version of the list used to conduct the card validity check be no more than one day old. Several commenters responded to this issue, and offered remarks relating to the use of MARSEC levels overall.

One commenter agreed with the Coast Guard's proposal to require, at a minimum, weekly updates of the CCL at MARSEC Level 1 and daily updates of the CCL at higher MARSEC levels.

Another commenter stated that we did not adequately clarify how different MARSEC levels would interact with Risk Groups A, B, and C. In response, we note that vessels and facilities that were proposed to be classified as Risk Groups B or C are not affected by this final rule, and that MARSEC interacts with Risk Group A as described in § 101.525. We have moved the MARSEC level requirements to this separate section to improve clarity.

Several commenters suggested that electronic TWIC inspection should only consist of card validation and card authentication at MARSEC Level 1, and that the Coast Guard should provide the flexibility for them to use electronic TWIC inspection for biometric matching purposes at higher MARSEC levels, or require it only at those levels. Other commenters recommended that electronic TWIC inspection should only be required once per day at MARSEC Level 1, with additional measures, such as full electronic TWIC inspection or random spot checks, implemented only at higher MARSEC levels. One commenter recommended that electronic TWIC inspection be used only at higher MARSEC levels, with visual TWIC inspections performed the rest of the time. We disagree with these suggestions. We believe that Risk Group A vessels and facilities should be secured at all times, not just at rare moments of heightened alert, and that biometric identification, one of the TWIC's strongest security features, should be used regularly. Based on the experience with the pilot, we also believe that consistency in electronic TWIC inspection processes is important, as varying use of security features can create confusion that can hinder operations.

One commenter suggested that the CCL should be updated daily at all MARSEC levels, not just at MARSEC Levels 2 and 3. Similarly, one commenter stated that the CCL should be continually updated at all times. The commenter stated that once an automated method is established to do this, there is no additional cost associated with the increased frequency. While we do agree that, if automated, it is simple to update the list of cancelled TWICs, we note that not all operators use an automated system at this time. While we realize that some larger operations can set up automatic updates of the list, other operations may need to conduct such updates manually. In our RA, we calculated that it takes 30 minutes to update the CCL. For that reason, we have only required in 33 CFR 101.525 that the list of cancelled TWICs be updated daily during periods of heightened risk according to the specified MARSEC level. We note that the required periods to update the list are considered minimum requirements, but operators are free to update more often if desired.

One commenter asked if electronic TWIC inspection requirements should be applied to Risk Groups B and C at higher MARSEC levels. We do not believe it should. This would require those vessels and facilities to purchase and install equipment for electronic TWIC inspection for use during those periods of heightened alert, dramatically increasing the costs of the rule for what we believe is, at this time, comparatively little corresponding benefit. Furthermore, changing electronic TWIC inspection procedures at irregular and long-spaced intervals can cause confusion that could impair operations.

4. Recordkeeping Requirements

In the NPRM, the Coast Guard proposed specific recordkeeping requirements relating to the use of TWIC readers in vessels and facilities. These proposals, in proposed §§ 104.235(b)(9) and 105.225(b)(9), specified that owners or operators must keep records of each individual granted unescorted access to a secure area, which would include the FASC–N, date and time that unescorted access was granted, and the individual's name (if captured). The NPRM also proposed to require that owners or operators keep documentation demonstrating that they had updated the CCL with the required frequency. The NPRM proposed a 2-year minimum retention time for such records, and specified that TWIC reader and PACS readers were sensitive security information (SSI), protected under 49 CFR 1520. We received several comments on the subject of recordkeeping, which are discussed below.

Many commenters suggested that the 2-year recordkeeping requirement was too long. One commenter supported the 2-year recordkeeping requirement, although noted that a shorter period would not be objectionable if the 2-year requirement was deemed overly burdensome or unnecessary. Another commenter suggested the period was an issue of concern, and that the Coast Guard should provide the rationale behind the requirement to retain records for 2 years rather than any other amount of time. The same commenter added that the argument for consistency with other recordkeeping requirements did not justify the burden of a 2-year requirement, although the commenter did not suggest an alternative timeframe. One commenter recommended that the records be retained for only 30 days, noting that this would be less burdensome.

In this final rule, as explained in more detail below, we are maintaining the 2-year timeframe for record retention as we do not believe it is unduly burdensome or unnecessary. We also disagree with the commenter that consistency with all other MTSA-related records is an insufficient rationale for requiring records to be kept for a 2-year period. We believe that if differing records were required to be kept for varying amounts of time, it would needlessly complicate the storage of those records and potentially add additional expenses.

One commenter stated that the 2-year retention period presents opportunities for the information to be mishandled or misused, and thus should be shorter, although no specific timeframe was suggested. While we realize that storing data for any period of time can result in misuse or mishandling, we note that the information is protected as SSI, and thus is subject to comparatively strict usage and storage controls. We believe that the risk of misuse or mishandling of the information is far outweighed by the security value of collecting and storing the data for use in security investigations. The commenter also stated that a shorter window would provide law enforcement sufficient data to assist in security investigation, but no alternative window was suggested nor supporting information supplied. Without additional information, we are not deviating from the 2-year period proposed in the NPRM and used in all other MTSA-related recordkeeping requirements.

This commenter also stated that 46 U.S.C. 70105(e) implies that information gathered by a TWIC reader from a worker's card must not be shared with an employer or otherwise publicly released. We do not believe that this characterization is correct. 46 U.S.C. 70105(e)(1) reads as follows: ''Information obtained by the Attorney General or the Secretary under this section may not be made available to the public, including the individual's employer.'' This restriction only applies to information obtained by the Attorney General or the Secretary, and includes information received by the Coast Guard. The information generated by electronic TWIC inspection is obtained by a private entity (the facility or vessel owner or operator) to whom the restriction in 46 U.S.C. 70105(e)(1) does not apply.

However, and as the commenter noted, some information collected by

the TWIC reader or PACS is considered SSI, and is thus protected from unauthorized disclosure under 49 CFR part 1520. The commenter recommended that the Coast Guard consider all electronic reader records, whether of an individual or of an aggregated group, be restricted to security use only and explicitly forbidden to be used in labor-management issues (such as establishing hours worked or reporting criminal activity).

Not all electronic reader records qualify as SSI and thus some information concurrently collected during electronic TWIC inspection can appropriately be used by an owner/operator for non-security but still legitimate purposes without violating 49 CFR 1520. The preamble of the NPRM contains clear guidance regarding the treatment of certain information collected by electronic TWIC inspection. In that document, we clearly stated that ''[w]e consider a TWIC-holder's name and FASC–N to be SSI under 49 CFR 15.5.'' We went on to explain that ''to the extent that a PACS contains personal identity [including the FASC–N] and biometric information, it contains SSI, which must be protected in accordance with 49 CFR part 15.'' [37] However, an important aspect of this final rule is that it allows electronic TWIC inspection to be integrated with a facility's PACS, which serves many other purposes beyond security and contains non-SSI information. For example, PACSs are legitimately used to restrict access for non-security purposes (such as private or dangerous areas) and to help establish the hours worked by employees. Owners and operators of facilities have valid uses for the non-private information not covered in the SSI regulations but still collected by a PACS regarding the location of personnel on their property.

One commenter requested specific information regarding the requirements established for owners or operators to secure the privacy of individual cardholders. We note that we have not established any new requirements in this rule for such safeguarding because the SSI requirements are already sufficiently comprehensive. See 49 CFR part 15 for regulations covering restrictions on disclosure, persons with a need to know, marking, consequences of unauthorized disclosure, and proper destruction of SSI.

The Coast Guard weighed privacy and security concerns in the development of this requirement. To minimize the amount of personally-identifiable information transferred from the TWIC to the TWIC reader, TWIC readers are specifically designed to only collect the minimum amount of information necessary to assist in access control and maritime security. Owners and operators who collect and maintain protected data from electronic TWIC inspections cannot share this information outside of their vessel or facility. The only allowable sharing is back to the TSA or to the Coast Guard for auditing or law enforcement purposes, or to assist with customer redress.[38]

Owners and operators are also bound by the restrictions on disclosure of SSI.[39] 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 the issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure, or of an order to cease future unauthorized disclosure.

Two commenters suggested that SSI requirements should not apply to electronic TWIC inspection records if no personally-identifiable information is recorded (*i.e.*, only the FASC–N, date, and time of the transaction is recorded). We note that pursuant to 49 CFR 1520.5(b)(11)(i)(A), SSI includes identifying information of certain transportation security personnel, which includes ''Lists of the names or other identifying information that identify persons as . . . having unescorted access to . . . a secure or restricted area of a maritime facility, port area, or vessel.'' This information is specifically addressed in the recordkeeping requirements of this final rule. For example, § 105.225(b)(9) states that the TWIC Reader or PACS system must capture the ''FASC–N, date and time that unescorted access was granted; and, if captured, the individual's name.'' If such information was captured, it would be considered SSI.

Commenters also suggested additional information that could be collected during electronic TWIC inspection. One commenter suggested that an electronic TWIC reader transaction should also include an identifier for the specific electronic reader device, and if it is a portable electronic reader, an identifier for the operator of the device. The commenter suggested that this information would enhance the usefulness of an audit trail. While we see that there could be some value in having this information recorded, we believe that it would be overly complex to add this information into the suite of recorded information at this time, and the value of such information would not be worth the additional cost. We note that such information might be gathered from other sources even without a requirement to collect it in this final rule. Nonetheless, should we reconsider the scope of data collection for electronic TWIC inspection in future rulemakings, we will consider this suggestion.

Two commenters recommended that recordkeeping requirements should be extended to situations where an electronic TWIC inspection is not used, such as visual TWIC inspections, RUA, and escorted access. One commenter suggested that without recordkeeping requirements for visual TWIC inspection, there is no incentive—other than avoiding the consequences of being caught—to actually conduct visual TWIC inspections. We disagree with these comments. A recordkeeping requirement for visual TWIC inspections would mean that each owner or operator would need to record information on each TWIC inspection. We would need to demonstrate that the cost of such a requirement is justified before imposing it on the regulated population. In that regard, we note that in 2013, the Coast Guard conducted 12,171 inspections at MTSA-regulated facilities for compliance with the regulations in 33 CFR part 105. As part of those inspections, Coast Guard personnel spot-checked 52,708 TWICs, finding a validity rate of greater than 97 percent. In light of the high validity rate, we do not believe that a recordkeeping requirement for visual TWIC inspections is appropriate or necessary.

One commenter also suggested that there should be recordkeeping requirements for when a person is granted unescorted access through the ''special circumstances,'' described in § 101.550 of the final rule, such as if he or she had reported their TWIC as lost or stolen. In the NPRM, we did not propose any requirements that records be kept for transactions that do not make use of electronic TWIC inspection. While such a suggestion is outside the scope of this final rule, we will consider it in future regulatory actions.

Furthermore, we are not creating new requirements for visual inspections in this final rule, including any recordkeeping requirements. This final rule pertains to requirements for electronic TWIC inspection. Requirements pertaining to other means of access, including access granted through visual TWIC inspection or escorted access to a secure area, are

[37] 78 FR 17806–7.

[38] *See* 49 CFR part 1520.

[39] *See* 49 CFR 15.9(a)(1).

outside the scope of the final rule. We do note that electronic TWIC inspection is a prerequisite for RUA, and thus a record is created when that transaction occurs. However, due to the nature of RUA, no additional records are kept outside of the electronic TWIC inspection transactions. Such recordkeeping would be burdensome and defeat the purpose of RUA.

One commenter suggested that the lack of criteria or specificity as to what the required records should contain severely limits their efficacy. We believe that the NPRM was clear on what records are required to be kept, but we will discuss them here in greater length. Specifically, a record should be kept of each instance in which a person is granted unescorted access to a secure area. This record must contain the FASC–N of the TWIC issued to the person granted unescorted access. If the TWIC reader or PACS captures the individual's name, the name associated with the TWIC must also be part of the record. Finally, the record must include the date and time the person was granted unescorted access (the time can be rounded to the nearest minute; it is not required that the precise second that access was granted be captured, although it is acceptable to be more precise). As noted in the NPRM, ''we allow individual regulated parties to determine the best method and manner of complying with the recordkeeping requirements.'' [40]

The commenter also requested additional justification for the 2-year period, stating that neither the argument for consistency nor the argument for law enforcement justify the length of time to hold records. As stated in the NPRM, the timeframe was designed, in part, for consistency with existing security-related and other recordkeeping requirements applicable to vessels and facilities, and we note that all other security recordkeeping requirements in the affected sections are subject to a 2-year retention period. In response to the commenters who requested additional justification, we would add that investigations of TSIs can involve analysis of data that stretches back for that amount of time, and we want to ensure that any historical data that could be useful is available. We believe that a 2-year period is an appropriate amount of time to ask owner operators to store data to ensure that no investigation is limited due to the unavailability of relevant data. We continue to believe that a uniform timeframe for recordkeeping requirements, when practicable, provides the most efficient regulatory system, and that the costs of storing data are minor compared to the security benefits provided.

The commenter also referred to the 2013 GAO report, noting its concern that the TWIC Pilot Program had difficulties collecting accurate, consistent data from the pilot sites.[41] While we are aware of the GAO's criticisms of the TWIC Pilot Program, we do not believe those data collection concerns are relevant to the data collection proposed by the implemented electronic TWIC inspection regulations. Beyond the fact that both involved data collections, the nature and uses of the data collected in the two programs are very dissimilar. For example, among many other items that related to the overall operation of the facilities at issue, the Pilot Program collected data on the number of people using TWIC readers, the amount of time taken per transaction, and the failure rates for transactions. These are very different data than collected by electronic TWIC inspection, which collects items such as the FASC–N. The data collected by electronic TWIC inspection is narrowly tailored to assist the Coast Guard and other law enforcement agencies in investigating TSIs, and the criticisms of data collection on the Pilot Report are not analogous.

One commenter stated that the recordkeeping requirements proposed in the NPRM would create a large amount of data and may need to be stored in a media that is not immediately accessible. The commenter requested that the final rule allow a reasonable amount of time to retrieve and produce the electronic records when requested. We agree with the commenter that a reasonable amount of time will be permitted to produce any requested records. This final rule deals only with recordkeeping requirements; it does not specify a timeframe for record retrieval.

One commenter requested clarification of a specific situation: a Port Authority operates a cruise terminal which uses an FSP, but when a cruise ship is in port, the cruise security line operates under its own FSP. The commenter asked who would be responsible for maintaining the records. Based on the information described in this situation, the owner or operator of the TWIC reader or PACS system conducting the electronic TWIC inspection would be responsible for maintaining the required records of those transactions. However, we note that recordkeeping requirements for any particular facility would be described in the FSP and that different situations may yield different results, but that these issues would be resolved during approval of the FSP.

Similarly, another commenter described a scenario where a private security company and a public entity share a facility. The commenter asked if the entities would need to share records. In response, we note that there is no requirement to share records, and that the owner or operator of the TWIC reader or PACS conducting the electronic TWIC inspections is the entity required to keep the records. Which entity is responsible for recordkeeping should also be addressed in the FSPs.

One commenter requested that, if a non-Risk Group A facility were to use electronic TWIC inspection on a voluntary basis, they should not be subject to the electronic recordkeeping requirements in proposed § 105.225(b)(9) and (c). Assuming that a facility is using electronic TWIC inspection on a voluntary basis to replace visual TWIC inspection, pursuant to the guidance in PAC 01–11, we disagree. If replacing security personnel with electronic TWIC inspection, then all elements of such an inspection, including recordkeeping requirements, would have to be met. Maintaining the electronic records as required provides additional security and information in case of a security breach in the future. Visual inspection programs are not required to maintain this type of information due to the large amount of time needed to manually enter the same information.

### *C. When To Conduct Electronic TWIC Inspection*

One of the areas in which the Coast Guard received the most comments on the proposed rule was the issue of when a TWIC must be read. Specifically, the NPRM used language that stated, ''prior to each entry, all persons seeking unescorted access to secure areas [must] present their [TWIC] for inspection before being granted such unescorted access'' (this language was used in proposed §§ 101.520(a)(1), 101.525 introductory text, and 101.530 introductory text).

Many commenters asked for clarification regarding this language, specifically relating to issues of where TWIC readers should be located, and to what specifically ''prior to each entry'' referred. Despite using identical language in the proposed regulatory

[40] 78 FR 17806.

[41] ''Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed'' (GAO–13–198) is available in the docket by following the instructions in the **ADDRESSES** section of this preamble.

text, the requirement for when to perform electronic TWIC inspection is very different for vessels than it is for facilities. With regard to vessels, we stated in the NPRM that ''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.'' [42] On the other hand, with regard to facilities, we stated that ''this NPRM proposes to require TWIC readers at the access points to each secure area,'' [43] which could necessitate a large number of TWIC readers in facilities like passenger facilities, many of which have multiple access points to secure areas within the facility. Similarly, the NPRM RA reflected this information, estimating that each facility might use a number of TWIC readers (passenger facilities, with many access points to secure areas, were estimated to require an average of 16 TWIC readers each), whereas each vessel might only be equipped with one or two, reflecting the fact that they would only be deployed at the entrances to the vessels, not at each access point to a secure area within the vessel.

Nonetheless, we recognize the confusion brought on by the proposed language. One commenter, for example, requested a clarification of the reference to ''each entry'' to a facility or vessel secure area. The commenter noted that passenger vessels and facilities included restricted areas, employee access areas, and passenger areas, and it was unclear from the NPRM where the electronic TWIC inspection requirements would be applied. In this final rule, we have used language that we believe more clearly describes the specific requirements of the rule. We broke the language down into two separate paragraphs, one for vessels (*see* § 101.535(a)), and one for facilities (*see* § 101.535(b)), using slightly different language for each. The final regulatory text for facilities now states, ''Prior to each entry *into a secure area of the facility,''* while the final regulatory text for vessels now states, ''Prior to each *boarding of the vessel.''* While the language is slightly modified, we believe it more clearly implements the proposed requirements in the NPRM.

**1. Secure, Restricted, Public Access, Passenger Access, and Employee Access Areas**

In terms of clarifying that an electronic TWIC inspection must be performed prior to each entry into a secure area (for facilities), we believe that it is important to clarify the term ''secure area,'' as well as explain the differences between secure areas and other types of areas on MTSA-regulated vessels and facilities. Many commenters asked questions that indicated the difference between secure areas, restricted areas, employee access areas, public access areas, and passenger access areas was not entirely clear. In this section, we discuss the definitions of these types of areas, given their definitions in 33 CFR part 101, as well as the additional explanation offered in NVIC 03–07 and other documents.

The statutory requirement for TWIC readers, stated in 46 U.S.C. 70105(a)(1), requires that anyone granted unescorted access to a secure area of a vessel or facility maintain a valid TWIC. Secure areas are defined in 33 CFR 101.105. The relevant portion of the definition states that ''*Secure area* means the area on board a vessel or at a facility over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard approved security plan. It does not include passenger access areas, employee access areas, or public access areas.''

The concept of a secure area is explained in more detail in NVIC 03–07, enclosure (3). Section 3.3b of that document explains that ''for facilities, the secure area is the entire area within the outer-most access control perimeter of the facility, with the exception of public access areas, and encompasses all restricted areas.'' Similarly, ''for vessels and OCS facilities, the secure area encompasses the entirety of a vessel or OCS facility, with the exception of passenger or employee access areas for vessels.''

Existing regulations distinguish between the secure area and areas designated as ''restricted.'' The term restricted area, as defined in existing 33 CFR 101.105, means ''the infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection [than secure areas].''

NVIC 03–07 also goes into detail explaining the difference between secure and restricted areas, noting that by virtue of the fact that the secure area encompasses the entire facility or vessel (with the exclusion of public, passenger, and employee-access areas), restricted areas fall within this perimeter.

Multiple commenters with facilities expressed concerns about the existence of multiple secure areas within any one facility, and what access control measures would be required by this final rule. Other commenters represented both vessels and facilities, but had similar concerns with regard to the differences among secure, restricted, and public access areas. The definitions of secure and restricted areas have implications when determining where to locate electronic TWIC inspection locations on various facilities. These locations would be marked in an FSP or a VSP. Given the requirement that electronic TWIC inspection be conducted ''prior to each entry'' into a secure area (for facilities), we would anticipate that the inspection points at facilities would be located at the access points to secure areas. For example, in a chemical cargo facility the entire facility may be considered a secure area, as security measures for access control may surround the entire facility. Such a facility would likely only conduct electronic TWIC inspection at the entrance to the facility. Alternatively, a facility might categorize the parking lot as a ''public access area'' so that employees and visitors can park, and electronic TWIC inspection could be conducted at the access point from the parking lot into the secure area of the facility. We note that a second round of electronic TWIC inspection is not required when passing from a secure area to a restricted area, although we would anticipate other security measures to be in place.

For passenger facilities, the majority of the areas may be designated ''public access areas,'' ''passenger access areas,'' or ''employee access areas'' (such as break rooms). In such an instance, electronic TWIC inspection points may only be located at entrances to secure areas such as the pier or FSO's office. The Coast Guard acknowledges the confusion surrounding this issue, which is why we have included a clarifying revision to 33 CFR 103.505, Elements of the Area Maritime Security (AMS) Plan, in which a parenthetical reference to the TWIC program may create confusion regarding whether TWIC provides access control for secure or restricted areas. This final rule creates electronic TWIC inspection requirements for access to secure areas, and does not address requirements for access control to restricted areas.

Finally, we note the concerns commenters had relating to secure areas on water. One commenter noted that the water where barge fleets are located is considered a secure area, but the area was only accessible by boat. The commenter questioned how electronic TWIC inspection could be conducted in such a situation. Similarly, another commenter requested that they be allowed to conduct electronic TWIC inspections on shore before entering

[42] 78 FR 17803.

[43] 78 FR 17803.

barge fleeting areas, as otherwise there would be no way to conduct an electronic TWIC inspection. Another commenter noted that the only ''access point'' into such secure areas may be a towing vessel with the dedicated purpose of guarding the area.

These commenters raise important issues as to how we would apply the electronic TWIC inspection process to secure areas on water, such as barge fleeting facilities. Upon consideration, we do not believe that requiring electronic TWIC inspection prior to entering such areas would be practical, as there is no particular access point to such an area that can be controlled by a TWIC reader. Electronic TWIC inspection would instead be required at the barge fleeting facility's shore side location.

Many commenters representing vessels were concerned about a situation involving a passenger vessel (potentially in Risk Groups B or C) with multiple secure areas and no one standing watch at the entrances to each secure area. We note that while the electronic TWIC inspection requirements are different for vessels than for facilities, the definitions of secure areas and restricted areas are similar. On non-passenger vessels, generally the entire vessel is considered a secure area. Certain areas within the vessel may have higher levels of security, and those would be considered restricted, which again are not impacted by this final rule. On passenger vessels, while security measures would still encompass the vessel, only certain areas would be considered secure, as passenger access areas and employee access areas are excluded from the definition of secure areas. As described below in Section V.C.2 of this preamble, because electronic TWIC inspection on vessels is only conducted when boarding the vessel, the exact location of secure and restricted areas on a vessel would not affect the placement of electronic TWIC inspection points.

a. ''Prior to Each Entry'' for Risk Group A Facilities

In this final rule, we are finalizing without change the proposed requirement that electronic TWIC inspection is required prior to each entry into a secure area of a Risk Group A facility. Similarly, we are finalizing the proposed requirement that electronic TWIC inspection is required prior to each entry onto a Risk Group A vessel. While some commenters objected to this policy, we believe that it represents the best balance of security and practicability at this time. Furthermore, we believe that many objections to the policy expressed by industry are addressed by clarifying that the new requirements apply only to Risk Group A vessels and facilities, and that vessels and facilities not in this group have no new requirements in this final rule. In this section, we address comments specifically related to Risk Group A facilities. Questions for Risk Groups B and C, as well as questions for vessels, are discussed in other sections of this preamble.

Several commenters requested guidance related to operations conducted under PAC 08–09, change 1. That document allows owners and operators of a vessel or facility to use a local access card to grant unescorted access to secure areas, assuming that the local access card is tied to a valid TWIC and that verification (visual or electronic) of the local access card is conducted each time access is granted to a secure area. Pursuant to PAC 08–09, TWICs needed only to be validated once every 24 hours. However, PAC 08–09 is only valid until the Coast Guard publishes a final rule requiring the use of TWIC readers as an access control measure.[44] Because this final rule establishes electronic TWIC inspection as a requirement for Risk Group A facilities, the guidance in PAC 08–09 will no longer be valid with respect to those facilities upon the effective date of this rule. Because there are no electronic TWIC inspection requirements for Risk Groups B and C, PAC 08–09 remains in force for those facilities. We intend to update PAC 08–09 before the effective date of this final rule.

We note that while PAC 08–09 will no longer be valid for Risk Group A facilities, the flexible performance requirements of this final rule will continue to allow access using local access or PACS cards, assuming the PACS is able to perform the electronic TWIC inspection requirements of biometric identification, the card validity check, and card authentication. While many commenters requested that Risk Group A facilities be permitted to continue to follow the guidance in PAC 08–09 (some of whom suggested that it could be augmented by a daily card validity check), we are not granting that request. Electronic TWIC inspection is a more secure system than that used under PAC 08–09 for a variety of reasons, but most distinctly because it performs a biometric identification each time a person is granted unescorted access to a secure area, whereas the system described in the PAC 08–09 does not. Biometric identification provides a higher level of certainty that an individual is an approved TWIC-holder than visual identification.

One commenter suggested that the purpose of TWIC is for a worker to be vetted, and that TWIC should not be used as an access control system, noting that it is up to the owner of the secure space to determine which TWIC-holders are granted unescorted access. While we agree that one of the benefits of TWIC is that it ensures an individual has undergone a background check, we disagree that vetting is the only purpose of a TWIC. Congress mandated that the TWIC contain the biometric identification of the TWIC-holder. Furthermore, Congress explicitly required that the Coast Guard ensure that only individuals who hold a TWIC be granted unescorted access to secure areas of MTSA-regulated facilities in 46 U.S.C. 70105(a)(1). We conclude, therefore, that it is the clear mandate of Congress for this biometric identification to be used to ensure that only TWIC-holders are granted unescorted access to secure areas of Risk Group A vessels and facilities. Using this function of the TWIC for identification verification purposes will enhance the security afforded by the TWIC program in the highest-risk areas.

Other commenters expressed the opposite view, arguing that the Coast Guard was wrong to limit the requirement of electronic TWIC inspection to Risk Group A vessels and facilities only. Multiple commenters suggested that the proposal to limit the use of electronic TWIC inspection to Risk Group A vessels and facilities deviated from Congress' intent in developing the TWIC program, and that to conform to the intent of Congress, we should have extended the mandate to perform electronic TWIC inspection to Risk Group B as well. Other commenters noted that in the ''findings'' section of the MTSA statute (Pub. L. 107–251, 101(11)), Congress found that ''[b]iometric identification procedures for individuals having access to secure areas in port facilities are important tools to deter and prevent port cargo crimes, smuggling, and terrorist actions.'' The commenter argued that to be responsive to Congress, TWIC cards should not be used primarily as a ''flash pass,'' but should be used more often as biometric identification tools.

The Coast Guard believes that the requirement instituted in this final rule represents a reasoned implementation of electronic TWIC inspection. As analyzed in the NPRM and associated preliminary RA, we believe the vessels and facilities in Risk Group A are at much greater risk than other MTSA-regulated vessels and facilities.

[44] PAC 08–09, change 1, p. 2.

Electronic TWIC inspection has a high utility in deterring and mitigating certain threats to these targets. Given the costs in infrastructure and operational needs associated with electronic TWIC inspection, as shown in the TWIC Pilot Program and in the Coast Guard's regulatory analyses, we do not believe that electronic TWIC inspection should be extended to other vessels or facilities at this time. Information and experience gained through the implementation of Risk Group A vessels and facilities will, however, help to determine whether and how the electronic TWIC inspection program should be expanded in the future.

Several commenters argued that the requirement to undergo electronic TWIC inspection prior to each entry into a secure area of facility was overly burdensome and unnecessary. One commenter stated that the Coast Guard does not understand the day-to-day operations of passenger vessels and facilities, and that only small areas are secure and restricted, requiring a TWIC-holder to move in and out of these areas multiple times per day. We disagree with this statement, and note that the NPRM and the NPRM RA repeatedly affirmed that a TWIC reader would be required at each access point to a secure area in a Risk Group A facility. We acknowledge that in cases where employees of a passenger facility move repeatedly from a non-secure area (such as a passenger access area) to a secure area, they will likely have to undergo repeated electronic TWIC inspections. We also note that these facilities already use access control measures to prevent unauthorized persons, including vessel passengers, from entering secure areas, and that this requirement only involves incorporating electronic TWIC inspection into those existing access control measures.

Other commenters also made suggestions that would allow for reduced numbers of electronic TWIC inspections for employees that enter and leave secure areas multiple times per day. Several commenters suggested that checking TWICs against the CCL multiple times per day is redundant, as the list is only updated, at most, once per day. These commenters suggested that at lower MARSEC levels, one electronic TWIC inspection per day would be enough, and then a visual TWIC inspection could be used for each subsequent entry into a secure area. We note that electronic TWIC inspection performs much more than just the card validity check, and that there is a need to check that the individual presenting the card is the correct individual presenting an authentic card each time he or she is granted unescorted access to a secure area. For these reasons, a single electronic TWIC inspection should not allow repeated grants of unescorted access to secure areas in Risk Group A facilities.

One commenter argued that its security needs would be better met through cross-checking TWICs via its employment, human resources, and internal security systems, and then issuing badges that it has control over. The commenter stated that in that situation, it would have the ability to verify and revoke access as necessary for the security of the facility. With the new flexibility for electronic TWIC inspection in this final rule, such cross-checking using facility-specific identification cards linked to a PACS is possible, as long as the facility's PACS performs the biometric identification, card validity check, and card authentication procedures required in this final rule prior to each entry into a secure area.

One commenter stated that the ''prior to each entry'' requirement is impracticable for cruise ship terminals. This commenter stated that dozens of porters, stevedores, and shore staff constantly move baggage in and out of secure areas using mechanical equipment such as forklifts and hand trucks, and that requiring electronic TWIC inspection at each entry would be potentially unsafe. We realize that there is a need to balance the requirement to ensure that only TWIC-holders are granted unescorted access to secure areas with the operational needs of a facility. In a situation such as that described by the commenter, an RUA plan could alleviate the burden of repeated and constant electronic TWIC inspections. The RUA option was designed primarily to address the needs of baggage handlers and stevedores, and was developed to facilitate operations such as those described by the commenter where persons must enter and exit a secure area on a continual basis. RUA is described in more detail in Section V.C of this preamble.

Several commenters were concerned that the proposed requirement for permanently placed TWIC readers at the access points for Risk Group A facilities offered no flexibility, and could restrict the use of portable TWIC readers as an option at less heavily-trafficked access points. We first note that the NPRM did not specifically require a fixed TWIC reader at all access points, but we assumed that many facilities would use fixed TWIC readers over portable ones at fixed access points for the purposes of analysis. However, we agree with the commenter that the NPRM did not offer enough flexibility, and thus this final rule adds another option for electronic TWIC inspection. Facilities will be able to use fixed electronic readers, portable electronic readers, or a PACS to conduct electronic TWIC inspection, depending on which works best considering their business operations.

One commenter raised a concern that a requirement to present a TWIC prior to each entry into a secure area would mean that TWIC-holders would have to carry their cards at all times, thus exposing cards to being damaged in a harsh environment or lost. The commenter recommended that a system be utilized that would allow them to keep their workers' TWICs in a safe and secure location where, upon request, the TWICs could be retrieved and inspected within a reasonable amount of time. We agree that this could be appropriate in many maritime environments, and thus the flexibility allowed by this final rule would permit such a system. A facility could control access to secure areas using a PACS to conduct the electronic TWIC inspection, thus allowing the TWICs themselves to be maintained in a safe, nearby location, where they could be inspected if necessary.

One commenter requested clarification with regard to overall personnel accountability within secured areas. Specifically, the commenter asked if the Coast Guard would require TWIC-holders to record when they exited a secure area, and if a facility should know who is in a secured area, at all times. In this rulemaking, we did not propose to require personnel accountability in this fashion, nor does the final rule require TWIC-holders to record when they exit a secured area. Another commenter expressed support for not proposing such a requirement in the NPRM. The final rule only requires electronic TWC inspection upon entering a secure area of a Risk Group A facility. With regard to recordkeeping, as discussed above, this final rule only requires that records be kept of individuals that enter the secure area, and of when they entered. This final rule does not require that records be kept of individuals leaving a secure area, nor does it require that records be kept of who is in a secure area at any particular time.

b. Recurring Unescorted Access

Many commenters requested that the Coast Guard reinstate the concept of RUA that had originally been considered in the ANPRM, but was not proposed in the NPRM. As described in the ANPRM, as part of an RUA plan, the owner or operator of a vessel or facility would conduct an initial biometric

match of the individual against his or her TWIC, either at hiring or upon the effective date of a final rule, whichever occurs later. This biometric match would include a verification of the authenticity and validity of the TWIC. Once this check is done, the TWIC would only be used as a visual identity badge, at a frequency to be approved by the Coast Guard in the amended security plan, so long as the validity of the TWIC is verified periodically, ranging from monthly to daily, depending upon Risk Group and MARSEC Level.[45] RUA, as described in the ANPRM, would be limited to 14 TWIC-holders per vessel or facility, although it was not clear whether that meant an RUA regime would only be approved if the vessel or facility crew were limited to 14 TWIC-holders, or if 14 people per vessel or facility would be exempted from electronic TWIC inspection procedures that would still be in place for other employees or persons seeking access.

The Coast Guard opted not to include RUA in the proposed regulatory text in the NPRM, despite the fact that many ANPRM commenters supported various versions of RUA procedures. In the NPRM, we explained that ''RUA was previously proposed [in the ANPRM] 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.'' [46] However, by limiting electronic TWIC inspection requirements to Risk Group A vessels only, and including the vessel crewmember exemption in the TWIC applicability section, we believed we had rendered the need for RUA as a mechanism for regulatory relief unnecessary. One commenter requested clarification about whether the proposed RUA mechanism would apply to facilities as well, or just vessels. While the NPRM did not explicitly discuss the use of RUA for facilities, we did not consider such plans viable. Unlike vessels, facilities regularly receive unfamiliar personnel, such as visitors, contractors, and deliveries, and must have a means to ensure those visitors are valid TWIC-holders, regardless of the size of the regular staff.

We received several comments in response to the decision in the NPRM not to include an RUA provision. Most commenters recommended that some sort of RUA provision be included in the final rule, although they differed in their interpretations of what, exactly, an RUA plan would entail. Furthermore, multiple commenters laid out specific examples of how RUA could improve operations in several scenarios. These comments are described below.

One commenter suggested that an RUA plan for vessel and facility operations, including operations at facilities that service passenger vessels, would require that a TWIC-holder undergo electronic TWIC inspection once when he or she reports for work each day. It was unclear from these comments specifically how this plan would be implemented. If RUA were limited to certain crewmembers or employees, it is unclear how those crewmembers would differentiate themselves from other TWIC-holders who would still be required to undergo electronic TWIC inspection prior to each entry into the vessel or into a secure area of the facility. Furthermore, unless all crewmembers or employees were subject to the RUA plan, it is unclear how such a system would reduce costs, as access control measures would still need to be in place that would need to differentiate between TWIC-holders and non-TWIC-holders, but also differentiate between those TWIC-holders granted RUA and those subject to repeated electronic TWIC inspection. These questions, along with the exemption from electronic TWIC inspection requirements for vessels with low numbers of crewmembers, are the reason that the RUA plan was not proposed in the NPRM, despite being raised in the ANPRM, and we still do not have clear answers to these issues.

Several commenters raised the issue of RUA with regard to certain port workers who repeatedly enter and leave secure areas, such as baggage porters at cruise terminals or workers such as stevedores transferring cargo into a secure area. Similarly, one commenter expressed concern about how porters would be able to do their jobs if required to conduct electronic TWIC inspection at each entry into the baggage area. Some commenters suggested that in order to permit workers to efficiently perform their jobs, which may entail entering and leaving a secure area several times an hour, biometric checks should be limited to the beginning of a shift and after extended breaks. The commenter stated that it is not operationally practical to have these workers undergo electronic TWIC inspection repeatedly.

We agree that, for narrow classes of vessel or facility employees such as baggage porters, the electronic TWIC inspection requirements could prove particularly burdensome, and that these workers could be accommodated using a limited form of RUA as suggested by the commenter. Some scenarios where this may prove useful include, for example, porters who carry baggage from a curbside check-in area (unsecure) to a baggage storage area (secure) for cruise customers, or forklift operators who transport packages from a loading area (unsecure) to a secure storage area on a vessel or facility. These persons need to travel back and forth across the secure-unsecure boundary repeatedly, and repeated electronic TWIC inspections can be both cumbersome and redundant in these situations.

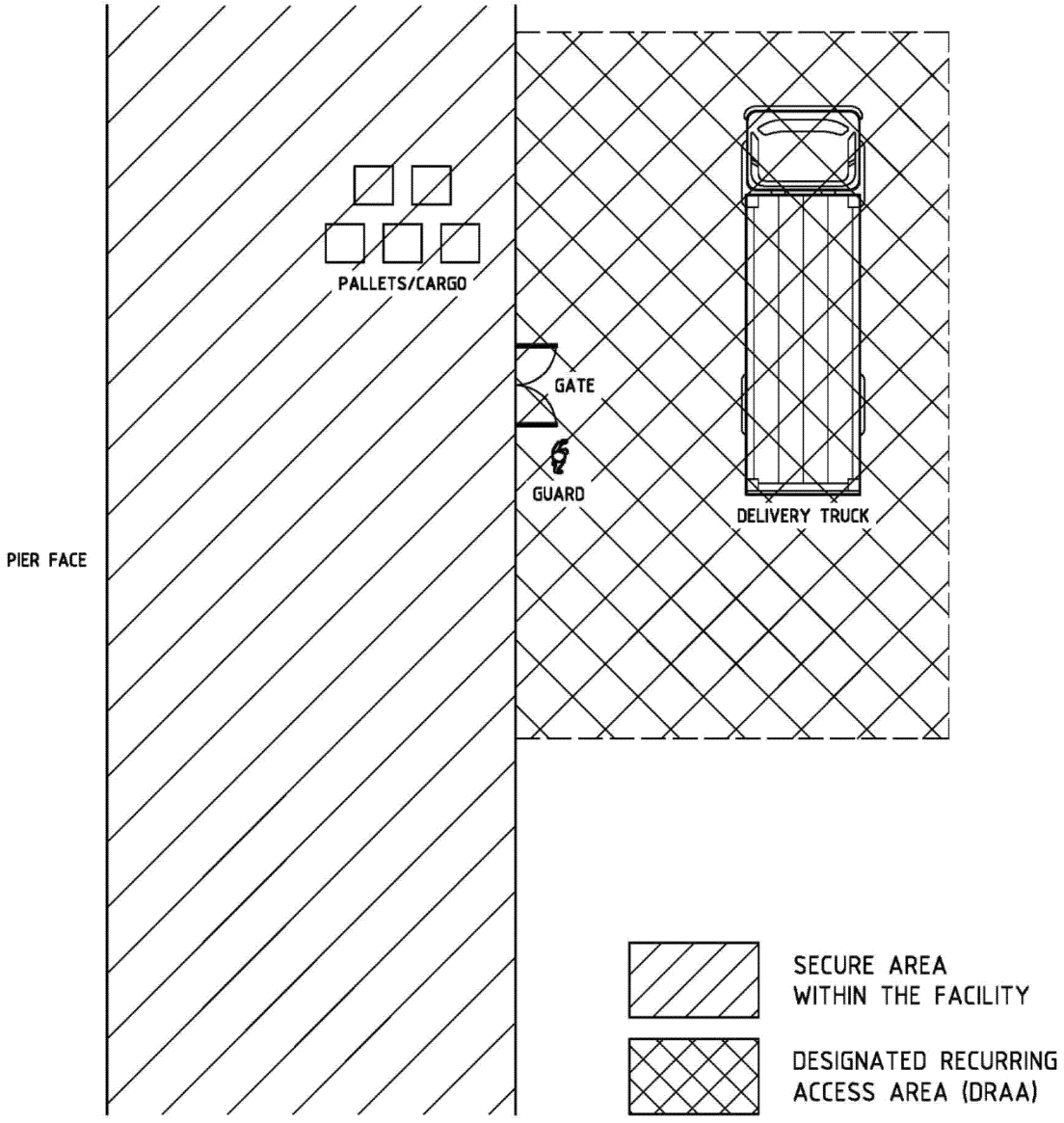
Therefore, to accommodate these situations without compromising security, we have added a limited form of RUA into this rule as § 101.555. The system would operate as follows: a vessel or facility would designate an area as a ''Designated Recurring Access Area (DRAA)'' in its security plan. As shown in Figures 1 and 2, the DRAA would consist of adjoining secure and unsecure areas, as well as the access gates between them. As long as a TWIC-holder stayed inside the designated area, he or she could pass between the unsecure and secure portions of the DRAA without having to undergo an electronic TWIC inspection each time he or she entered the secure portion.

[45] *See* 74 FR 13362.

[46] *See* 78 FR 17804.

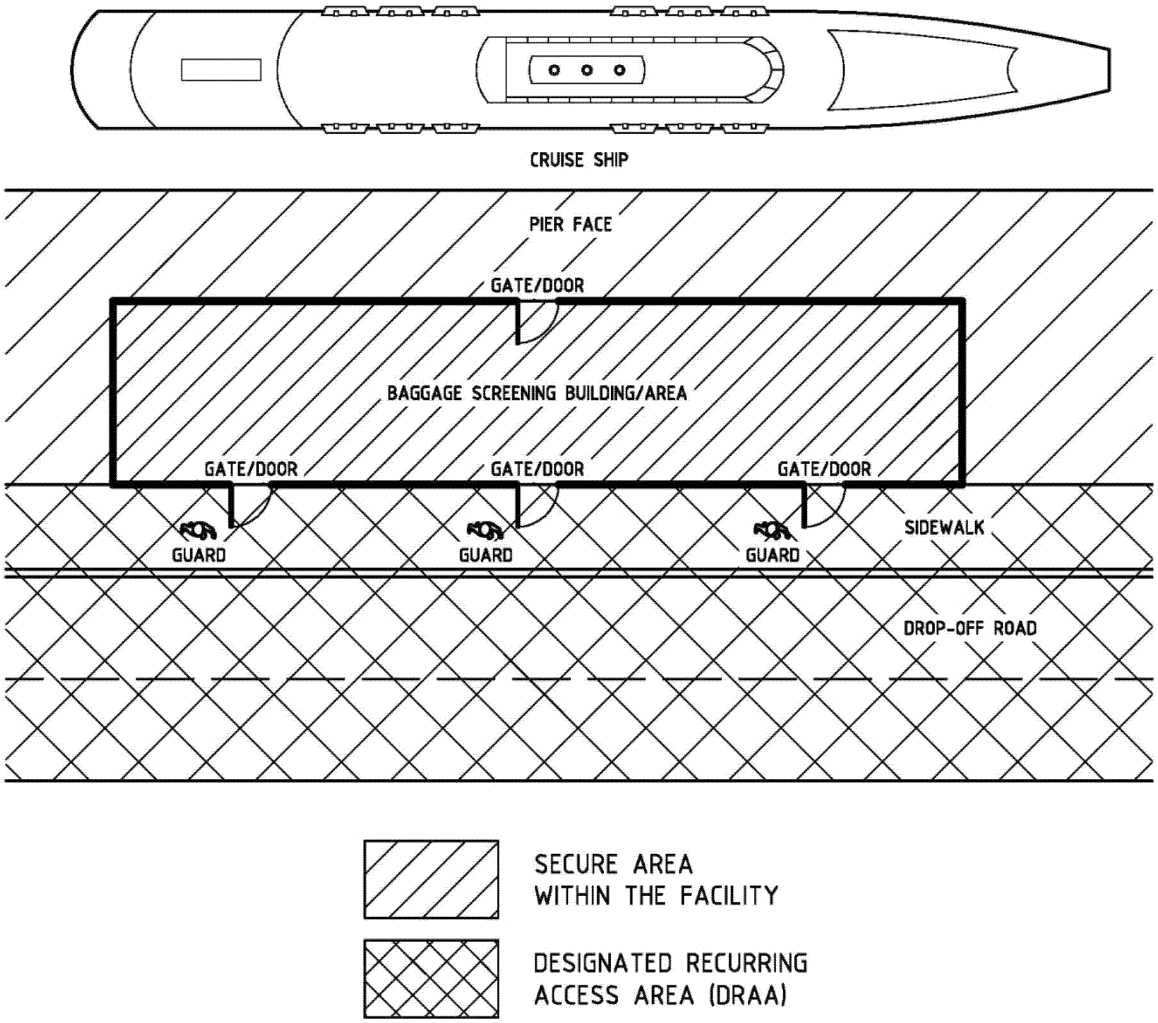
BILLING CODE 9110–04–P

Figure 1: Designated Recurring Access Area (DRAA): Facility




DELIVERY TRUCK ACCESS

Figure 2: Designated Recurring Access Area (DRAA): Vessel




BILLING CODE 9110–04–C

We have considered the problem of differentiating between those persons granted recurring access and those who must undergo electronic TWIC inspection prior to each entry. Certain restrictions and conditions would be applied to ensure that no unauthorized persons gain access to the secure area through the DRAA. In order to allow recurring access, the Coast Guard is requiring that security personnel be present at the access points to the secure areas where recurring access is used. Although electronic devices, such as TWIC readers or a PACS reader, can be used to control access at other entrances, in an RUA situation the TWIC (or a linked PACS card) is not presented at each entry to the secure area. Instead, the presence of security personnel is necessary to properly control access while allowing the known DRAA participants to pass through repeatedly.

An additional requirement for a DRAA is that the entire unsecured area must be visible at all times to the on-site security personnel. This requirement is necessary to ensure that all recurring access participants have undergone the necessary electronic TWIC inspection before entering a secure area. We believe that without this requirement, it might be possible for a non-TWIC-holder to ''talk their way'' into a secure area by claiming they had already undergone a TWIC inspection, and had merely returned from an authorized break. We note that among various GAO criticisms of the maritime security program, this was one of the means by which GAO investigators were able to bypass security measures. We agree with one commenter that suggested electronic TWIC inspection should be repeated once returning from a break. By requiring recurring access participants to stay within sight of the security personnel or undergo a new electronic TWIC inspection, we can ensure that these types of incidents do not happen.

To gain recurring access, a TWIC-holder would need to undergo

electronic TWIC inspection, including biometric matching, the first time the TWIC-holder entered the secure portion of a DRAA. This would of course happen at the beginning of a work shift, but would also happen after each time the TWIC-holder left the DRAA for any reason, including administrative reasons, lunch breaks, or even to use the restroom. We have also added a provision that requires at least one electronic TWIC inspection per change of security personnel in order to account for shift changes.

We have attempted to make the RUA policy as flexible as possible while still maintaining security. We note that the use of a DRAA is a wholly voluntary option, and that access to secure areas of a vessel or facility may always be accomplished through the procedures in §§ 101.535 and 101.550. Even within a DRAA, only access points that are used for recurring access must be manned by security personnel, so there can be other access points controlled by unmanned means (such as a lock connected to a TWIC reader) for employees who do not need recurring access. Furthermore, an area can be designated a DRAA at certain times. For example, at a cruise ship terminal, a curbside area could be designated a DRAA only during boarding times. This would allow the access points to be secured by unmanned means during other periods when recurring access is not necessary.

We also note that a DRAA may be incorporated in a Joint Vessel and Facility Security Plan, allowing an area where employees can cross from a pier to a vessel repeatedly without having to undergo electronic TWIC inspection each time. This can facilitate the loading or unloading of vessels considered secure areas.

2. Risk Group A Vessels

We received fewer comments regarding the requirements for electronic TWIC inspection for Risk Group A vessels than for vessels in other Risk Groups. In the NPRM, we discussed the TWIC reader requirements as applied to the Risk Group A vessel population in Section IV.L, ''Physical Placement of TWIC Readers.'' In that section, we stated that ''[w]e 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.'' [47] We realize that this sentence may have been confusing, as the only proposed modification to § 104.265(a)(4) was to add the sentence ''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'' to the existing requirement that the owners or operator of a vessel must ensure that only authorized TWIC-holders are granted unescorted access to secure areas of the vessel.[48] A clearer citation would have been to § 101.514(a)(1), which contained the proposed requirement that prior to each entry, all persons seeking unescorted access to secure areas in Risk Group A vessels and facilities must present a TWIC. The regulatory text was also unclear about what ''prior to each entry'' meant, and many commenters believed that it meant prior to each entry into a secure area of the vessel, which was contrary to the stated intent of the preamble.

As stated above, in this final rule, we are modifying the electronic TWIC inspection requirements so that they are both more flexible and more performance-oriented than described in the NPRM. In this final rule, we require electronic TWIC inspection rather than the presentation of a TWIC. Furthermore, again as stated above, we are clarifying the language relating to the locations of electronic TWIC inspection. The new language, contained in § 101.535(a), ''Requirements for Risk Group A Vessels,'' reads ''prior to each boarding of the vessel.'' We believe that this change should improve the clarity of the regulatory text.

The Passenger Vessel Association (PVA) noted the confusion between the preamble and regulatory text, noting in its comments that ''The proposed rule states (proposed § 104.265(a)[49]), 'Prior to each entry, all persons must present their TWICs for inspection using a TWIC reader.''' The PVA argued that ''[t]he Coast Guard's explanatory material in the **Federal Register** suggesting otherwise cannot override the very clear language of the proposed regulation.'' We agree that the language is confusing, and have clarified it appropriately. The commenter also recommended that the Coast Guard adopt a version of RUA that would allow a single verification of the TWIC status when the TWIC-holder reports to the secure area for the first time each day. While this was not what RUA, as proposed in the ANPRM, was intended to do, we note that the clarified electronic TWIC inspection requirements in this final rule will result in far fewer inspections on vessels than the commenter anticipated.

One commenter, who operates as a combined ferry/terminal operator, discussed methodologies to improve security through a ''Combined Security Plan'' that allowed them to effectively identify risk while allowing their employees to perform their duties in a secure and efficient manner. The commenter suggested that its ferries have multiple points of access from the terminal to the ferry as well as multiple points of access to secure areas within the ferry. The Coast Guard agrees that insofar as security measures between a terminal and ferry can be combined, a combined plan can produce a more effective and efficient security regime than separate plans. Furthermore, secure areas within terminals can be connected to the entrances of ferries. In those instances, where TWIC-holders pass directly from a secure area of the terminal onto a ferry, an additional electronic TWIC inspection is unnecessary. For that reason, we interpret the phrase ''prior to each boarding of the vessel'' in § 101.535(a)(1) to include the situation in which an electronic TWIC inspection has been carried out prior to boarding a ferry, and the TWIC-holder has not entered an unsecure area in the interim. We believe that such an allowance will reduce the costs of compliance with the electronic TWIC inspection program for combined ferry/terminal operators without compromising security.

Several commenters posed questions relating to a situation in which a Risk Group A vessel, such as a ferry, has multiple secure areas separated by unsecure areas, but sole control of its terminal facilities. These commenters asked whether it would be possible to have only one TWIC reader at each terminal facility for both vessel and facility workers. As explained below, such a system could meet the requirements for electronic TWIC inspection. If a worker is granted unescorted access to a secure area of a Risk Group A facility, and remains in the secure area, he or she may board a Risk Group A vessel without a second electronic TWIC inspection. We note that once on board a Risk Group A vessel, a worker does not need to undergo additional electronic TWIC inspections when entering secure areas.

One commenter stated that vessels at sea should be required to update the CCL if there are separate and distinct secure areas on board the vessel. We disagree, and note that the requirement for Risk Group A vessels is that

[47] 78 FR 17816

[48] 78 FR 17830–17831, Amendatory Instruction 16a

[49] We note that the language cited is actually from proposed § 101.520(a)(1), not § 104.265(a).

electronic TWIC inspections are only performed when the personnel are boarding the vessel, not, like facilities, at each entry into a secure area. Therefore updating the CCL while at sea would not serve any functional purpose.

3. Risk Groups B and C

In this final rule, we are completely removing any mention of additional TWIC requirements for vessels and facilities other than those covered under § 101.535, ''Electronic TWIC inspection Requirements for Risk Group A.'' Many commenters noted the apparent differences between the language on Risk Groups B and C in the NPRM preamble and the proposed regulatory text in §§ 101.525 and 101.530, which pertained to Risk Groups B and C respectively.

In the preamble of the NPRM, we stated that we were making no changes to either of those groups. For example, in Section III.E.7.b of the NPRM, ''Risk Group B TWIC Reader Requirements,'' we stated that ''proposing requirements for Risk Group A only in this NPRM is indicative of our desire to minimize highest risks first. . . .'' [50] Likewise, in Section III.E.8.b, ''Risk Group C TWIC Requirements,'' we noted that ''Under current regulations (which would not change under this NPRM) for vessels and facilities categorized in this NPRM Risk Group C, security personnel must visually inspect the TWIC of each person seeking unescorted access to secure areas.'' [51] Our preliminary RA echoed this language. In that document, we did not include any cost analyses relating to vessels or facilities in Risk Groups B or C.

However, as commenters noted, in proposed §§ 101.525 and 101.530, we included language from the ANPRM that contradicted the statements in the preamble that no new requirements were being proposed for Risk Groups B and C. The proposed regulatory text would have required vessels and facilities in Risk Groups B and C to undergo visual TWIC inspection prior to each entry into a secure area. Thus, the practical effect of such a requirement would have been to require security personnel be posted at each entry point, which many commenters argued would dramatically increase the compliance costs for MTSA-regulated vessels and facilities in Risk Groups B and C, contrary to the stated intent of the regulation. The specific comments are described in greater detail below.

We received a large number of comments from the owners and operators of passenger vessels that would have been categorized as Risk Groups B and C. These individuals suggested that the proposed regulatory text would impose severe burdens on their operations, burdens that would be extremely costly and produce relatively little in the way of security benefits. The PVA's comment summed up many of its members' statements, noting that ''Group B and C passenger vessels and facilities have multiple and widely separated secure areas with large public access areas in between. TWIC-holders move regularly in and out of those spaces multiple times during the day. As a practical matter, this means that in those vessels and facilities, there must be some other person stationed in or outside of each secure area to visually inspect the TWIC and presumably bar the holder from entry if the visual inspection is unsatisfactory.'' [52] We agree with the PVA that, with regard to passenger facilities, the wording of the proposed regulatory text could have had this effect, but these concerns are moot because we removed the proposed provisions on Risk Groups B and C.

Many operators of passenger vessels argued that the requirement to visually inspect TWICs at each entry point into a secure area would be enormously expensive, impracticable, and provide little security benefit. One commenter suggested that the use of existing access control systems on vessels could be used in place of visual TWIC inspection on vessels. One commenter wrote, ''we do not have enough berthing to add 2 additional people that would do nothing but sit at the galley door on opposite shifts and request to see the TWIC card of [the] same person multiple times per day.'' [53] Another commenter wrote that requiring a visual TWIC inspection at each entry to a secure area on a vessel ''is a bit like asking your brother who lives in your household for his ID whenever he needs to use the restroom.'' [54] Commenters also argued that needing to present a TWIC to enter an unmanned engine room space could hinder access in an emergency. Many other commenters echoed the substance of these remarks. In this final rule, we hope to clarify that: (1) With regard to Risk Group A vessels, the requirement to undergo electronic TWIC inspection applies only upon boarding the vessel, and (2) there are no new requirements, for either visual or electronic TWIC inspection, or anything else applicable to vessels or facilities outside of Risk Group A in this final rule. The existing visual TWIC inspection requirements in 33 CFR Chapter I, Subchapter H continue to apply to vessels and facilities outside of Risk Group A.

We received similar comments pertaining to Risk Group B and C facilities. Many commenters requested that the final rule should state that approved FSPs using PAC 08–09 practices continued to be allowed for Risk Group B and C facilities. We reiterate that this final rule imposes no changes on the operation of Risk Group B or C facilities; accordingly, such practices will continue to be allowed. One commenter suggested that the guidance permitting voluntary use of TWIC readers, contained in PAC 01–11, be continued for Risk Group B and C facilities. While that guidance is rendered obsolete by this final rule, we note that its contents have been largely incorporated into the final rule as § 101.540, which permits non-Risk Group A facilities to use electronic TWIC inspection procedures in lieu of visual TWIC inspection on a voluntary basis.

One commenter recommended that language be added to proposed § 101.525 (Risk Group B) that would allow a PACS card to be used in place of a TWIC at each entry to a secure area. Some commenters noted that the PAC 08–09 practices are significantly less costly than inspecting a TWIC at each entry into a secure area. While the rule imposes no new TWIC inspection requirements on Risk Groups B or C, we follow this suggestion with regard to Risk Group A facilities in the form of increased flexibility for electronic TWIC inspection. One commenter added that this could be coupled with a periodic TWIC check to ensure it is still valid. We note that Coast Guard inspections, conducted at Risk Group B and C facilities, accomplish exactly this check.

4. Miscellaneous Questions Regarding the Locations of Electronic TWIC Inspection

In this section, we address certain questions raised by commenters on issues related to the locations where electronic TWIC inspections must take place. Several similar comments asked us to clarify what an ''access point'' to a secure area is. The commenter provided an example of an alarmed fire escape door that leads to a pier, which is designated as a secure area. In response, we would clarify that an ''access point'' is any location where personnel access from a non-secure area to a secure area is permitted, in any circumstance, by a facility's security plan. However, we agree with the commenter that requiring an electronic

[50] 78 FR 17802.

[51] 78 FR 17803.

[52] USCG–2007–28915–0190, p. 12.

[53] USCG–2007–28915–0139.

[54] USCG–2007–28915–0215, p. 3.

TWIC inspection in the event of a fire would be unwise. For that reason, we are including language in § 101.535(e), allowing an exemption from electronic TWIC inspection requirements for emergency situations. We believe that this exemption will protect against unauthorized access to secure areas without compromising safety in the event of an emergency response.

The commenter also provided an example of a roll-up baggage door, where the porters bring in luggage they collect from guests at the curb in front of a cruise ship terminal. Next to the roll-up door is ''a typical personnel door.'' The commenter asked if the two doors count as a single access point, or if they are two separate access points, where each door requires its own TWIC reader. Again we note that in this final rule, we are not requiring the installation of TWIC readers; instead the requirement is that prior to being granted unescorted access to a secure area, an individual must undergo electronic TWIC inspection. Thus, two doors to a secure area could be controlled by a single TWIC reader or PACS reader, if permitted in the FSP.

The commenter also asked about an area that switches between being secure and non-secure based on the operations taking place there at a given time. In such an instance (and permitted, we assume, by the FSP), when the area is designated secure, persons would need to undergo electronic TWIC inspection before being granted unescorted access. At times when the area was designated non-secure, there would be no such requirement. We would expect the relevant FSP to contain more detail on how such an area would operate.

D. Determination of Risk Groups

The third major area of comments related to the determination of which vessels and facilities should be placed into which Risk Groups. In §§ 104.263 and 105.253 of the NPRM, we proposed three different Risk Groups, A, B, and C, although there were no differences between the requirements for Risk Groups B and C. The proposed Risk Groups were as follows:

Risk Group A:

- Vessels certificated to carry more than 1,000 passengers;
- Vessels that carry CDC in bulk;
- Vessels engaged in towing another Risk Group A vessel;
- Facilities that handle CDC in bulk;
- Facilities that receive vessels certificated to carry more than 1,000 passengers; and
- Barge fleeting facilities that receive barges carrying CDC in bulk.

Risk Group B:

- Vessels that carry hazardous materials, other than CDC, in bulk;
- Vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues;
- Vessels certificated to carry 500 to 1,000 passengers;
- Vessels engaged in towing a Risk Group B vessels;
- Facilities that receive vessels that carry hazardous materials, other than CDC, in bulk;
- Facilities that receive vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues;
- Facilities that receive vessels certificated to carry between 500 and 1,000 passengers;
- Facilities that receive vessels subject to 46 CFR chapter I, subchapter D, that carry any flammable or combustible liquid cargoes or residues;
- Facilities that receive a vessel engaged in towing a Risk Group B vessel; and
- All OCS facilities subject to 33 CFR part 106.

Risk Group C:

- Vessels carrying non-hazardous cargoes that are required to have a VSP;
- Vessels certificated to carry fewer than 500 passengers;
- Vessels engaged in towing a Risk Group C vessel;
- Facilities that receive vessels carrying non-hazardous cargoes;
- Facilities that receive vessels certificated to carry fewer than 500 passengers; and
- Facilities that receive vessels towing a Risk Group C vessel.

Most comments were related to the categorization of vessels and facilities in Risk Group A, with many commenters requesting clarification on how to classify their own facilities, or offering rationales for why vessels and facilities should be categorized differently. As stated in previous parts of this discussion, the NPRM did not propose any additional requirements for Risk Groups B or C, and thus, for purposes of the electronic TWIC inspection requirements, whether or not a vessel or facility is classified as Risk Group A is the only relevant distinction.

In this final rule, we have made a number of modifications to the classification of facilities and vessels in response to the comments. The major changes are summarized as follows:

- We have changed the crewmember exemption cutoff for vessels from 14 crewmembers to 20 crewmembers, as well as clarified how to calculate the number of crewmembers to apply this exemption.
- We have removed the specific reference to barge fleeting facilities from the Risk Group A classification, and now treat barge fleeting facilities like all other MTSA-regulated facilities.
- We have eliminated the distinction between Risk Groups B and C. Vessels and facilities are now classified as either Risk Group A or non-Risk Group A.

1. Risk Group A Facilities

In the NPRM, we defined Risk Group A facilities in proposed § 105.253(a) as: (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. We developed Risk Group A, along with the other Risk Groups, using a risk-based analysis system that identified which types of facilities were exposed to the most risk in the event of a TSI. This system used the MSRAM to derive a numeric ''consequence'' for a class of facilities. Once the potential risk to a class of facilities was ascertained, we then determined whether a program of electronic TWIC inspection would provide utility in alleviating that risk. This analysis is described in far greater detail in the ANPRM[55] and the NPRM,[56] and we refer interested parties to those documents for a detailed discussion.

Several commenters raised issues relating to the fundamental nature of our analysis, arguing that certain factors, such as the geographic location of a facility or its proximity to higher-risk facilities should have been incorporated into our analysis. After considering the comments, we have decided to largely retain the overall structure of how Risk Group A is structured. The basis for the analysis is discussed in Section V.A, above.

Several commenters suggested that the MSRAM analysis used by the Coast Guard to determine Risk Group A was flawed, and that a different methodology to determine the Risk Groups should have been employed that would bring more facilities into the Risk Group A category. Many of these commenters recommended that the Coast Guard adopt a risk analysis approach that focuses on area risks or geography, rather than the risks associated with classes of facilities. For example, one commenter recommended that the risk analysis should have included the risk to port operations where the port has minimum channel depth, or for petrochemical facilities that would create a significant impact to

[55] 74 FR 13363.

[56] 78 FR 17810.

commodity supplies, or chemical facilities where an attack could have significant environmental consequences.

Other commenters recommended that the Coast Guard consider the geographic area surrounding a facility as the most important factor in determining the appropriate Risk Group. Similarly, another commenter stated that the Coast Guard should expand the risk-based concept and aggregate risks to the port area first, before using MSRAM to determine specific risks. In response, the Coast Guard considered a broad range of factors, including geographic location, when determining the Risk Groups. The totality of that analysis identifies the highest risk vessels and facilities.

One commenter stated that the Port of New York is the nation's highest-risk port, suggesting that TWIC inspection should also be used to mitigate risks associated with criminal activity such as drug trafficking, cargo theft, and alien contraband smuggling. The commenter suggested that TWIC readers should be required at more facilities in that port than are required under this rule. We are not requiring electronic TWIC inspection as a crime prevention measure, and we reiterate that the primary purpose of requiring electronic TWIC inspection is not to prevent crime, but to prevent TSIs at high-risk vessels and maritime facilities.

One commenter stated that MSRAM does not contain any data that identifies TWIC readers as a threat mitigation tool, and that assumptions must have been made that would connect the MSRAM data with mitigation scenarios based on TWIC readers. In response, as emphasized throughout this preamble, an electronic TWIC reader is a threat mitigation tool because it provides identity verification, card authentication, and card validity checks more effectively than visual TWIC inspection. In the MSRAM context, a target's ''vulnerability'' is defined as the probability that an attack will be successful. MSRAM measures target vulnerability as a product of three factors: (1) Achievability, which assumes the absence of all security measures and then factors in the degree of difficulty delivering an attack on a target; (2) Target Hardness, which considers the probability that the attack focal point would fail to withstand the attack; and (3) System Security, which considers the probability of a security strategy in place to successfully thwart an attack before it occurs. Electronic TWIC inspection is a component of System Security.

Some commenters argued that the relative locations of Risk Group A and B facilities should factor into the risk analysis. One commenter stated that the NPRM did not consider a scenario where a Risk Group B facility is immediately adjacent to a Risk Group A facility. The commenter suggested that a terrorist could use a counterfeit TWIC to gain access to the Risk Group B facility (which would conduct only a visual TWIC inspection), and then use the location to mount an attack on the adjacent Risk Group A facility. Other commenters echoed the sentiment, stating that a Risk Group B facility that is immediately adjacent to a Risk Group A facility should not automatically have less stringent requirements that could become a threat vector.

While we agree that this specific scenario was not used in our analysis, we also do not believe that it would be appropriate to consider. We note that in this scenario, all the counterfeit TWIC accomplishes is to allow the adversary to get to the perimeter of the Risk Group A facility. If the Risk Group B facility was not located in the adjacent location, then it would be even easier for the terrorist to get to the aforementioned perimeter. Electronic TWIC inspection is designed to thwart access to the secure area of Risk Group A facility, not to prevent access to the secure perimeter.

One commenter recommended that large container terminals should not be classified as Risk Group B, but rather as Risk Group A. The commenter stated that a disruption of operations at any one of these facilities could have a significant impact on the economy, and that the Coast Guard should have used secondary consequences in its economic analysis. While we agree that a disruption of a large container terminal could have significant economic impacts, we disagree with the suggestion that container facilities should be automatically classified in Risk Group A. As stated elsewhere in this preamble, MSRAM considers scenarios associated with threats to container facilities. However, for the purpose analyzing electronic TWIC inspection, we limited our consideration to attack scenarios that require physical proximity to the intended target. Controlling access to a target is an essential component of security from such attack scenarios because access control helps to detect and perhaps delay the attackers before they reach the target. Threats to cargo containers are typically not attack scenarios that require physical proximity to the intended target. Accordingly, electronic TWIC inspection would not mitigate such threats. Such threats are addressed in existing Coast Guard regulations (33 CFR 104.275 and 105.265) that specifically require owners and operators to implement detailed security measures relating to cargo handling on vessels and at facilities.

a. Alternative Security Programs

One commenter, representing the American Gaming Association, recommended that instead of the risk categorization approach proposed in the NPRM, the Coast Guard should adopt a case-by-case approach to classification of facilities participating in its Alternative Security Program (ASP). This commenter noted that the security measures adopted on these vessels and facilities can be more restrictive than Coast Guard regulations require, and that those vessels and facilities should not be required to use TWIC readers. Furthermore, the commenter stated that the TWIC reader technology may be duplicative with systems onboard gaming vessels. We disagree, for the reasons stated above, with using a case-by-case approach to risk categorization rather than the Risk Group system proposed in the ANPRM and NPRM. However, we note that several suggestions that the commenter made are permitted by this final rule. If the existing security system on a vessel or facility is duplicative of a TWIC reader (*i.e.,* is capable of conducting a card authentication, card validity check, and biometric match), then a dedicated TWIC reader would not be required. We believe that a PACS can be modified to meet these requirements with relatively little additional costs, as discussed in the accompanying RA.

Similarly, several commenters stated that the combined vessel and facility security plan, as adopted in the PVA ASP, should permit facilities to be exempt from electronic TWIC inspection requirements if the vessels they service are exempt. For reasons discussed below, we disagree. We note that all ASPs, including the PVA ASP, can be used to integrate security between passenger terminals and vessels, but that the ASP must meet all electronic TWIC inspection requirements in this final rule.

b. Determining Risk Group A Facilities

Several commenters asked questions or requested clarifications of issues related to whether certain facilities would be classified as Risk Group A facilities. Our thoughts on these specific questions are below:

One commenter requested clarification regarding a cruise terminal

that handles general cargo (presumably not including bulk CDC) when cruise ships are not present. The commenter asked whether a Risk Group A classification would only apply to a facility when a passenger vessel certificated to carry 1,000 or more passengers was at the facility. In such an instance, movement between Risk Groups would be permissible, if detailed in the FSP in accordance with 33 CFR 105.253(b). One commenter suggested that allowing movement between Risk Groups would be unfair to those facilities that have installed electronic TWIC inspection technology. We disagree, and note that when subject to Risk Group A electronic TWIC inspection requirements, a facility would have to make full and complete use of such technology, and would incur all the costs of installing the technology.

One commenter requested clarification that a facility would not be classed as a Risk Group A facility if it handles multiple passenger vessels not in Risk Group A simultaneously. This is correct, a facility (assuming, of course, that does not handle or receive vessels carrying CDC in bulk) would only be classified as Risk Group A if it handles one or more vessels certificated to carry over 1,000 passengers. The relevant risk factor is the presence at the facility of a vessel certificated to carry more than 1,000 passengers. The relevant risk factor is not the mere presence on the facility of more than 1,000 people, which would be a transient event driven by simultaneous arrivals.

Several commenters requested clarification of the use of the word ''handle.'' Proposed § 105.253(a)(1) categorizes facilities that handle CDC in bulk as Risk Group A facilities, but commenters had questions about how to interpret this phrase. These commenters requested clarification on how a facility would be classified if a vessel carrying CDC in bulk were to stop at a facility, but not transfer any of the bulk CDC cargo there. After considering the comments, and to clarify risk groups, we have determined that any facility that handles or receives vessels carrying CDC in bulk will be classified as Risk Group A. While moored at a facility, a vessel must rely on the facility's security program to adequately secure the interface between the facility and vessel and mitigate the threat of a TSI. For that reason, the facility should conduct electronic TWIC inspection to meet the security needs associated with handling or receiving vessels that carry CDC in bulk.

Discussions at public meetings prompted the Coast Guard to clarify the term ''handle'' as it related to non-maritime commerce. Specifically, the question was raised whether a facility would be classified as Risk Group A if it was used to transfer CDC in bulk through rail or other non-maritime means. In this situation, such a facility would be considered to ''handle CDC in bulk'' and would be classified as Risk Group A. This is because the bulk CDC would be on the premises of a MTSA-regulated facility, and thus the facility's access control system would need to be used to mitigate the risk of a TSI. We note that there are provisions where non-maritime activities of a facility can be located outside of the facility's MTSA footprint. In that situation, where the bulk CDC is not a part of the maritime transportation activities, it may be that a facility could define its MTSA footprint in such a way as to exclude that area. In such a case, the TWIC reader requirements that are being implemented in this final rule would not apply in that area.

Several commenters also requested clarification of the term ''in bulk.'' The term ''bulk'' or ''in bulk'' is defined in the Coast Guard's existing MTSA regulations (33 CFR 101.105) as meaning ''. . . a commodity that is loaded or carried on board a vessel without containers or labels, and that is received and handled without mark or count.'' Additionally, the term ''bulk'' is defined in 33 CFR 126.3 as ''. . . without mark or count and directly loaded or unloaded to or from a hold or tank on a vessel without the use of containers or break-bulk packaging.'' To clarify, the use of hoses and conveyor or vacuum systems would be considered direct loading or unloading and thus involve ''bulk.'' We have added such language to the definition of ''bulk'' in § 101.105 to improve clarity. We have also removed the phrase ''on board a vessel'' from the definition of ''bulk or in bulk'' to avoid confusion. Specifically, as stated above, a MTSA-regulated facility would be classified as Risk Group A if it handled bulk CDC offloaded by a train or other non-maritime means. A MTSA-regulated facility that handles or receives bulk CDC is determined to be Risk Group A whether or not the facility accepted the bulk CDC from a vessel. Finally, one commenter requested clarification that container terminals do not carry CDC in bulk. While we can clarify that CDC shipped in containers would not be considered bulk CDC, we note that some container facilities may also handle CDC in bulk.

Some commenters requested clarification of the term ''receive,'' in regards to what the requirements would be if a Risk Group A vessel were received by a Risk Group B facility. The term ''receive'' is used in this final rule only in § 105.253(a)(2), which states that ''facilities that receive vessels certificated to carry more than 1,000 passengers'' are considered Risk Group A. In this instance, the word ''receive'' means that the vessel moors or transfers passengers to or from the facility. If there is a need for such a passenger vessel to moor up or transfer passengers at a non-Risk Group A facility, the COTP would need to be contacted to ensure that proper security measures are in place.

One commenter asked how Strategic Ports would be classified. A Strategic Port designation, which means the location is used by the military to load equipment, has no direct impact on the electronic TWIC inspection requirements. Individual vessels and facilities will be required to comply with the applicable parts of this regulation based on their specific operations.

One commenter asked if facilities that receive vessels certificated to carry more than 1,000 passengers would be classified as Risk Group A if all the vessels the facility received are exempted from the electronic TWIC inspection requirements by virtue of having fewer than 14 crewmembers. The commenter further stated that it is rare that the vessels certificated to carry more than 1,000 passengers ever carry that many, and that there are rarely 1,000 passengers in the facility. Regardless of this fact, pursuant to § 105.253(a)(2), such a facility would be required to conduct an electronic TWIC inspection prior to each entry into a secure area of the facility. We note that neither condition the commenter discussed is grounds for classifying the facility as anything other than Risk Group A. The fact that the vessels are exempt from the electronic TWIC inspection requirement due to their low manning requirement does not grant a TWIC exemption to the facility, for reasons discussed in greater detail below.

Furthermore, the fact that the ferries at issue ''rarely'' carry the number of passengers they are certificated to carry does not change the status of the facility either. Our analysis has shown that the class of facilities that receive large passenger vessels present a heightened risk of a TSI, and that the use of electronic TWIC inspection in such facilities is an effective means to mitigate that danger. We believe that the access control requirements in this rule represent a good balance between costs and security.

Several commenters were concerned that the dichotomy between electronic TWIC inspections on vessels and facilities could present problems for mariners. One commenter called a situation ''absurd'' where a ferry terminal, servicing ferries certificated to carry over 1,000 passengers, would be required to meet electronic TWIC inspection requirements, while the ferries themselves would be exempt from those requirements due to their low crew size. We disagree with the commenter's characterization of the regulations. Ferry terminals that handle large ferries present a risk of a large-consequence TSI, so much so that we believe that requiring a biometric identification before granting an individual access to the non-passenger areas of the ferry terminal is a warranted security burden. On the other hand, we do not believe that electronic TWIC inspection is necessary to gain access to the ferries themselves, considering that non-TWIC-holding passengers will also have access to the same vessels. Contrary to the commenter's assertion, we believe it is quite reasonable to only require electronic TWIC inspections when the TWIC-holder is accessing an area where non-TWIC-holders are excluded. As we stated previously, the electronic TWIC inspection requirements are designed in such a way as to only require a burden where the security benefits will be tangible and substantial, which is why they apply as they do.

Some commenters suggested that where the presence of, and access to, CDC in bulk can be isolated from areas not containing these products within a large MTSA footprint, the facility should be allowed to limit elevated security measures to the higher-risk area only. This is a subject that was also raised in the NPRM.[57] Upon consideration, and given the general flexibility accorded by this final rule, we believe that this suggestion is appropriate. If bulk CDC is contained in a discrete area of the facility, it may be possible to isolate that area from other areas of the facility. Any areas where bulk CDC is transferred, passed through, or stored (permanently or temporarily) would be subject to the electronic TWIC inspection access control requirements. If the owner or operator of a facility were to take this approach, we would still consider the facility a Risk Group A facility. However, the owner or operator would be permitted to delineate in the FSP a portion of the facility as not subject to the electronic TWIC inspection requirements. The FSP would also have to contain details of how unescorted access to other secure areas is still limited to TWIC-holders.

Finally, many commenters presented examples of specific situations where they believed that electronic TWIC inspection in parts or in all of their facilities was inefficient or redundant. With regard to those situations, 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 and 105.130, as appropriate. We have endeavored to tailor these requirements to be as effective as possible, but certain situations must be dealt with on an individualized basis.

One commenter in a public meeting asked the Coast Guard to consider an exemption for LNG/LPG facilities not conducting transfer operations. Similarly, this commenter and others requested an exemption for cruise ship terminals when vessels are not present at the terminal. Without specific information, we cannot comment on the likelihood of a waiver, but note that in certain circumstances, facilities can change Risk Groups depending on operational needs.

One commenter in a public meeting stated that container facilities should not be considered CDC facilities, and would therefore not be in Risk Group A. Given the definition of ''in bulk'' provided in 33 CFR 101.105, any CDC being transported in a container (including tank containers) would be considered packaged and thus would not cause the facility to be classified as Risk Group A. We note that if a container facility were also used to transfer or store bulk CDC, it would be considered a Risk Group A facility and thus subject to electronic TWIC inspection requirements.

2. The Crewmember Exemption Does Not Apply to Facilities

Many commenters supported the Coast Guard's proposal to exempt vessels with 14 or fewer crewmembers, but felt that a similar exemption should be applied to facilities with 14 or fewer employees as well. For the reasons described below, we disagree with this concept and are not including an exemption for small facilities similar to the exemption for low-crew vessels.

One reason not to expand the electronic TWIC inspection exemption to facilities is due to the specific language of the SAFE Port Act. As stated above, the vessel exemption is predicated on Section 104 of the SAFE Port Act, codified in 46 U.S.C. 70105(m)(1), which prohibits the Coast Guard from requiring the placement of an electronic reader on a vessel unless the vessel has more individuals on the crew that are required to have a TWIC than the number we determine warrants such a reader. No similar mandate exists regarding facilities.

Secondly, we believe that the nature of access to facilities is fundamentally different from the nature of access to vessels, and thus the rationale that justifies an exemption for vessels with a low crew count does not transfer to facilities with a low employee count. As stated elsewhere in this preamble, the TWIC serves fundamentally different roles with regard to facilities and vessels, due to the nature of the respective populations. On vessels (with the exception of passenger vessels), everyone on the vessel is generally known to one another, and new persons are generally not introduced to the vessel population while at sea. For this reason, the electronic TWIC inspection requirements for vessels, when applied, require only that the electronic TWIC inspection occur when boarding the vessel, not prior to each entry into a secure area of the vessel (such as an engine room). Conversely, at facilities, the entrance, exit, and egress of persons who are not employees is a regular occurrence; drivers, contractors, pedestrians, mariners, and other non-employees are on facility grounds regularly. Indeed, truck drivers make up one of the largest populations of TWIC-holders. For this reason, there are many persons on facility grounds that are not ''known'' to facility employees, and so additional security measures must be employed to ensure that unescorted access to the secure areas of a facility is granted only to TWIC-holders. For Risk Group A facilities, we believe that the appropriate level of security is to conduct an electronic TWIC inspection of each individual before granting them such access. That is why electronic TWIC inspection at facilities is required ''prior to each entry into a secure area,'' rather than only at the perimeter of the facility,[58] as is the case with vessels. Due to the differences in electronic TWIC inspection requirements, we do not believe an exemption from the electronic TWIC inspection requirements based on a low number of employees is appropriate for Risk Group A facilities.

One commenter, in addition to requesting the extension of the low crewmember exemption to facilities, specifically requested that barge fleeting facilities with 14 or fewer people be excluded as well. In this final rule, barge fleeting facilities are no longer a

[57] 78 FR 17797.

[58] *See* § 101.535(b)(1).

separate class of facilities specifically subject to electronic TWIC inspection requirements. However, barge fleeting facilities are treated as facilities, and are subject to the same electronic TWIC inspection requirements as other facilities.

3. The Low Number of Crewmembers Exemption

The NPRM proposed that, unlike facilities, vessels in Risk Group A are exempt from the electronic TWIC inspection requirements unless they have more than 14 TWIC-holding crewmembers. This exemption was based, in part, on the statutory limit imposed in the SAFE Port Act, 46 U.S.C. 70105(m)(1), which prohibits the Coast Guard from requiring the placement of an electronic reader on a vessel unless the vessel has more individuals on the crew that are required to have a TWIC than the number we determine warrants such a reader. In the ANPRM and the NPRM, we tentatively proposed that this number would be 14 crewmembers, basing our recommendation on an analysis conducted by the Towing Safety Advisory Committee (TSAC). For the final rule, factoring in comments received and assumed risks, we have increased this number to 20 crewmembers.

We received numerous comments on the proposal to exempt all vessels with 14 or fewer TWIC-holding crewmembers from the electronic TWIC inspection requirements. In the NPRM, we requested that commenters explain any alternative suggestions and provide available data to support their comments. Comments we received generally fell into two categories. Many commenters suggested different numbers for the exemption threshold, with a fair majority supporting a larger number, thus exempting more vessels from the electronic TWIC inspection requirement. The other main group of commenters requested clarification on how, specifically, we would calculate the crew size of any particular vessel to determine whether a Risk Group A vessel would be exempt from the electronic TWIC inspection requirements. Both items are discussed below.

4. Calculating the Total Number of TWIC-Holding Crewmembers

Several commenters raised questions as to how, specifically, the Coast Guard would calculate the number of TWIC-holding crewmembers on a vessel to determine whether the vessel would be exempt from the electronic TWIC inspection requirements. Upon review, we found that there was some degree of confusion with regard to how this number is determined. We have identified two approaches to calculating the exemption number that may have led to this confusion. One approach would be to calculate the number by counting the total number of persons employed as crewmembers on the vessel. The NPRM's original determination of 14 crewmembers was calculated using this approach. That number included the Master, Chief Engineer, and three four-person rotating crews. We counted the total number of persons employed as crew, whether or not all of them would serve together simultaneously.

The other approach would be to calculate the number by referring to a vessel's Certificate of Inspection (COI) regarding crew size, which does not contain information regarding multiple crew rotations, but rather just the manning requirements for the vessel. Using that methodology, the same vessel described above, with a Master, Chief Engineer, and several four-person rotating crews would actually have had six crewmembers. As explained more fully below, this final rule adopts the latter approach.

Commenters also put forth a number of detailed issues relating to how the number of crewmembers would be determined. One commenter noted that while at any given time during a shift, the total number of required TWIC-holders aboard will generally be 14 or fewer, during shift changes the number will swell to more than 14. The commenter went on to question the definition of the term ''crewmember,'' noting that there may be TWIC-holders on board, such as security personnel, who are not members of the marine crew required under the vessel's COI. The commenter requested that the Coast Guard clarify the scope of the 14-crewmember exemption with regard to TWIC-holders who are not members of the marine crew.

Similarly, several commenters specifically requested that the Coast Guard clarify that the 14-crewmember threshold only includes the required number listed on the vessel's COI, and does not include ''persons in addition to the crew,'' industrial workers, etc. Some commenters recommended that for uninspected vessels, ''required crew'' should include all personnel assigned to the vessel performing navigation, safety, and security functions. Commenters also asked whether crewmembers included additional individuals such as company representatives, cadets, and contractors. One commenter stated that 46 U.S.C. 2101(21) excludes certain company representatives from being counted as passengers, so they could be counted as crew. Also, in situations where a vessel is forced to carry persons other than crew, such as emergency responders, commenters asked if they would still be subject to the exemption from the electronic TWIC inspection requirement.

In response to these comments, the Coast Guard is providing additional detail and explanation regarding this exemption. Based on our own analysis, and on the comments received, we agree with the commenters who suggested that ''crewmembers'' should include all personnel required to hold a TWIC in the required manning section of the COI (and we note that there are no uninspected vessels subject to MTSA requirements). Other persons in the crew section and the ''persons in addition to the crew'' section of the COI do not count towards the calculation for total number of TWIC-holding crewmembers. We reached this decision for the following reasons.

First, whether a vessel is subject to electronic TWIC inspection requirements should not vary based on transient circumstances, such as whether a company representative is on board, or a crew change causes the number of TWIC-holders on the vessel to temporarily swell and exceed the threshold. Electronic TWIC inspection programs must be incorporated into a security plan and followed consistently. We believe that the stability from having a consistent electronic TWIC inspection process will help serve the goals of the inspection requirements while minimizing the burden on vessels and facilities in Risk Group A.

Second, establishing the minimum manning requirement as the threshold number helps to ensure that other manning decisions are not affected by the electronic TWIC inspection requirements. For example, if it were based on the total number of employed crew, irrespective of whether that crew was required for manning the vessel, then some owners or operators of vessels might choose to lower their staffing requirements rather than introduce the new procedures. We received several comments suggesting that certain companies might choose to eliminate staff rather than comply with electronic TWIC inspection requirements. Tying the electronic TWIC inspection requirements to the minimum manning requirements will significantly reduce the risk of this occurring. The minimum manning requirements of a vessel are tied to the intrinsic nature of the vessel, and are not nearly as elastic as the other crewing needs of the vessel.

5. Threshold for the Crewmember Exemption

Based on the TSAC recommendation, we proposed in the NPRM that the cutoff number of crewmembers that make a vessel exempt from the electronic TWIC inspection requirement should be 14. We specifically requested comments from the public on whether 14 is an appropriate cutoff number, and requested explanations and available data to support any arguments for alternative numbers. We received numerous comments regarding this issue. Some commenters suggested that 14 was an appropriate number, but the majority suggested that it be increased.

The PVA and other commenters suggested that the Coast Guard should not have followed TSAC's recommendation, as not all sectors of the domestic maritime industry have input into that group's recommendations. The PVA suggested that 20 was a more appropriate number, noting that the largest minimum manning requirement for its members' vessels was 16. This figure is larger than 14, but not so large that long-time crewmembers would not recognize each other. This figure was suggested as appropriate because it would be a figure developed with the consultation of industry.

Similarly, many passenger vessel operators suggested that the exemption threshold be set high enough to exempt passenger vessels. One commenter suggested that the threshold number of 14 did not make sense, and that even with a crew of 20–30 people, it would be impossible for an imposter amongst them to go unnoticed. Another commenter suggested that 40 crewmembers would be a better threshold, arguing that the regulatory compliance costs of electronic TWIC inspection, added to other costs relating to security, were too onerous.

After considering all comments, we have decided to increase the number to 20 crewmembers as the figure for determining the threshold number under 46 U.S.C. 70105(m). Considering input received from all areas of industry, we believe it is an appropriate crew size at or under which all crewmembers will be able to quickly identify people who do not have unescorted access to secure areas. We realize that this may be a conservative figure, and that there is no hard number at which all crewmembers will recognize each other by sight. This number is highly dependent on the length of time the crew has served together, and on the reliability of every individual crewmember's memory. Nonetheless, we believe that the figure of 20 crewmembers presents a reasonable threshold at which all members of the crew can be realistically be expected to recognize one another. However, we are continuing to study the issue, and may propose to expand the electronic TWIC inspection requirements by reducing the exemption threshold in a future rulemaking.

The Coast Guard realizes that increasing the crewmember threshold now exempts not only most passenger vessels, but many vessels that carry CDC in bulk. We are comfortable with this exemption at this time for two reasons. First, as stated by many of the commenters, we believe that a crew of 20 on a vessel that carries CDC in bulk will all be familiar with one another, so the risk of an unauthorized person being unnoticed on the vessel is slim. Second, due to the requirements for electronic TWIC inspection at the facilities where the CDC vessels conduct a majority of their business, the vast majority of these crewmembers will have their TWIC verified when passing through the facility on their way to the vessel, during crew changes or other trips ashore. Finally, one commenter in a public meeting noted that TWIC readers on vessels may be exposed to explosive atmospheres, and that therefore, TWIC readers must be intrinsically safe. In the event that TWIC readers are installed in hazardous areas, they would need to comply with all applicable requirements associated with those areas, which would at the minimum likely entail additional costs for testing and certification, and we note that no TWIC reader on the QTL is currently certified as intrinsically safe. For these reasons, we believe that imposing an additional requirement that crewmembers undergo an additional round of electronic TWIC inspection each time they board the vessel would provide limited security value for vessel with fewer than 20 crewmembers carrying bulk CDC.

6. Outer Continental Shelf Facilities

In the NPRM, we proposed to characterize all OCS facilities as Risk Group B, meaning that they would not need to undertake electronic TWIC inspection. In this final rule, the Coast Guard continues to exclude OCS facilities from electronic TWIC inspection requirements. One commenter, an owner of some OCS facilities, asked whether TWIC readers could be placed at ''the point(s) of embarkation'' as opposed to placing TWIC readers on the OCS facility itself. Such a placement would be permissible if described in an approved FSP. However, we note that because OCS facilities are not considered Risk Group A, no electronic TWIC inspection requirements will apply as a result of this final rule.

7. Vessels and Facilities Not in Risk Group A

Many commenters supported the Coast Guard's decision not to include additional requirements for Risk Groups B and C in the NPRM. We appreciate the support, and agree that at this time, only vessels and facilities in Risk Group A will be affected by the electronic TWIC inspection requirements in this final rule. However, as stated in the NPRM, this final rule ''should not be read to foreclose revised TWIC reader requirements in the future.'' [59] Many commenters took this, and similar statements, as an indication that we had planned to extend electronic TWIC inspection requirements to Risk Group B vessels and facilities. As a result, we received several comments on the categorization of vessels and facilities within those Risk Groups.

One commenter suggested that all facilities, including those proposed to be in Risk Groups B and C, should be required to have at least one portable TWIC reader. The commenter stated that this would allow the facility to complete a comprehensive check of a TWIC, which would help to deter potential attackers by making it more likely that they would be caught. While we agree that adding electronic TWIC inspection to all facilities would produce a security benefit, for the reasons extensively detailed in this rulemaking, we do not believe that such measures would be efficient at this time for lower-risk facilities. The commenter also argued that security guards should not manually check the CCL during visual TWIC inspection, as it could distract him or her. We note there are no requirements to check the list of cancelled TWICs during visual TWIC inspection, nor does this rulemaking affect visual inspection procedures.

One substantial change being made in this final rule is the discontinuation of the distinction between Risk Group B and Risk Group C. The distinction between these two Risk Groups was relevant in the ANRPM, where we had proposed that Risk Group B vessels and facilities would be required to use TWIC readers on a random basis, whereas Risk Group C vessels and facilities would not be required to use TWIC readers at all. However, in the NPRM, we proposed to eliminate the random TWIC screenings from the Risk Group B requirements, and thus there was no distinction in

[59] 78 FR 17790.

requirements between those two Risk Groups. Nonetheless, we still proposed that the terminology for Risk Groups B and C be included in the regulations. Despite the lack of distinct requirements, many commenters read the NPRM to mean that electronic TWIC inspection requirements would be applied in some manner to Risk Group B vessels and facilities, and many commenters discussed the criteria by which vessels and facilities were classified as Risk Group B or C.

One commenter did not support the proposed placement of Oil Spill Response Vessels and Oil Spill Response Barges in Risk Group B, arguing that these vessels carry primarily an oily water mixture, rendering them at low risk for terrorist attack. The commenter provided additional analysis distinguishing Oil Spill Response Vessels from tank vessels, and requested that they be classified as Risk Group C.

Multiple commenters supported the decision to place Offshore Supply Vessels in Risk Group C, but wanted to clarify the definition of ''Offshore Supply Vessel'' for the purposes of TWIC requirements.

One commenter argued against the placement of all OCS facilities in Risk Group B. The commenter believed they should be subject to the same site-specific analysis that other facilities are subject to, and placed into Risk Group B or C as appropriate.

Several commenters responded to the Coast Guard's request for information as to whether petroleum refineries and storage facilities should be categorized as Risk Group A. Some commenters stated that it would be inappropriate for the agency to arbitrarily re-categorize these facilities without supporting study and analysis, and requested that if the Coast Guard omitted a risk in its initial analysis, a second notice and comment opportunity should be provided. One commenter noted that, according to the Coast Guard's RA, the risk level for petroleum facilities was more comparable to Risk Group C than Risk Group A. Commenters also noted that due to the spacing of petroleum tanks at facilities, it is highly unlikely that a fire at one tank could ''jump'' to another.

Several commenters provided the Coast Guard with a 2008 study entitled ''Risks Associated with Gasoline Storage Sites,'' which they argued demonstrated that gasoline does not pose a high risk of off-site consequences if involved in an incident, particularly one related to security.

One commenter expressed concern about the expectation regarding the phase-in statements made in the NPRM, stating that the absence of ''definitive statements'' has left the owners and operators of facilities in Risk Groups B and C wondering what will happen and what they should do.

Similarly, one commenter stated that it seemed as if ''phased in'' was already the basic approach being taken by the Coast Guard, and that revisions to the electronic TWIC inspection requirements were all but certain. That commenter requested that instead of this approach, the Coast Guard should specifically identify the vulnerabilities that will be addressed and develop a proposal accordingly. Finally, commenters noted that if the Coast Guard were to propose expanding electronic TWIC inspection requirements beyond Risk Group A, a new Regulatory Flexibility Act analysis would be required.

One commenter drew a distinction between petroleum refineries and petroleum storage facilities. The commenter stated that the petroleum storage facilities only store petroleum, whereas refineries may contain many types of more hazardous materials, such as hydrogen, although the commenter also stated that such facilities are well-equipped to handle those materials.

Based on the comments received on this issue, we are not categorizing petroleum storage or refining facilities as Risk Group A in this final rule. Furthermore, we note that if and when the Coast Guard decides to propose additional electronic TWIC inspection requirements for facilities not currently classed as Risk Group A, global factors such as the cost of implementing electronic TWIC inspection, risk factors relating to the threat of a TSI, or other unforeseen conditions may have changed, necessitating a reconsideration of which vessels and facilities should be subject to additional security measures. The factors raised by commenters will be considered if and when additional TWIC inspection requirements are proposed in the future.

We agree with the argument put forth by commenters that before extending electronic TWIC inspection requirements, a revised analysis of the costs and benefits should be undertaken and that opportunity to comment on those proposed requirements should be provided. Given the arguments raised in the comments, it is clear that more analysis needs to be conducted before the requirements of electronic TWIC inspection are extended to vessels and facilities not in Risk Group A. We do not believe that setting out the risk parameters for the next group of vessels and facilities to which electronic TWIC inspection may be applied is appropriate at this time. If and when the electronic TWIC inspection requirements are phased in further, the Coast Guard believes that the additional flexibility afforded by not having preset definitions for the lower-tier Risk Groups will allow us to better tailor the future rulemakings appropriately. As the analysis of risks, threats, and costs continues to evolve, we will conduct further analysis as appropriate as well as solicit additional information from the public.

8. Barge Fleeting Facilities

The inclusion in Risk Group A of barge fleeting facilities that handle barges carrying CDC in bulk was a topic discussed by a large number of commenters. The Coast Guard received comments from a variety of barge fleet operators, towing operators, and trade associations. Universally, comments on this subject argued that barge fleeting facilities should not be required to install TWIC readers. For the reasons described below, based on the comments received, we have removed the separate requirement that barge fleeting facilities that handle barges carrying CDC in bulk are specifically considered Risk Group A. Instead, barge fleeting facilities are considered facilities, and may be required to perform electronic TWIC inspection if the standard criteria for Risk Group A are met.

Barge fleeting facilities are defined in 33 CFR 101.105 as ''a commercial area, subject to permitting by the Army Corps of Engineers . . . or pursuant to a regional general permit[,] the purpose of which is for the making up, breaking down, or staging of barge tows.'' Because this rulemaking would only affect barge fleeting facilities that interact with barges carrying CDC in bulk, only those barge fleeting facilities which are used for the staging of barge tows would be affected by this final rule. In the NPRM, we proposed that all barge fleeting facilities that service barges carrying CDC in bulk would be considered Risk Group A.

Comments on why barge fleeting facilities should not be included in Risk Group A fell into four general categories. First, many commenters argued that the cost of installing TWIC readers at barge fleeting facilities would be higher than the installation costs at other facilities due to their remoteness, and that the Coast Guard's preliminary RA had not taken this into account. Second, several commenters argued that due to the remote location or lack of permanent infrastructure of many barge fleeting facilities, the consequences of a TSI would not be so great as to warrant

an inclusion into Risk Group A. Third, one commenter argued that because barge fleeting facilities only service vessels that would be exempt from the TWIC reader requirement (because they have fewer than 14 crew), the facilities should also be exempt. Finally, several commenters argued that a TWIC reader would not enhance security at barge fleeting facilities. We address each of these comment categories below.

The cost of installing TWIC readers at barge fleeting facilities was cited by commenters as a reason to reconsider placing them in Risk Group A. Commenters generally argued that logistical considerations made installing TWIC readers in barge fleeting facilities substantially more expensive than at traditional installations. Several commenters stated that infrastructure costs, such as electricity, Internet access, and a facility to protect the TWIC reader would cause this requirement to be dramatically more expensive than originally considered. Similarly, commenters stated that these costs were not considered by the Coast Guard in its preliminary RA. Multiple commenters stated that the $300,000 initial phase-in costs estimated for bulk liquid facilities seemed like a low estimate. These commenters suggested that they would refuse to handle barges carrying bulk CDC rather than bear this increased cost, and that a final rule would cause rates to rise at other facilities. Similarly, commenters suggested that the decision to require TWIC readers at these barge fleeting facilities could actually be detrimental to security because, building on the idea that many facilities would refuse to handle bulk CDC barges, those barges would become concentrated at the few facilities that did allow them, thus increasing the risk profile of the fleeting areas that service them.

We disagree with the notion that TWIC readers would be substantially more expensive to operate at barge fleeting facilities than at other types of facilities. As summarized above, the commenters who made this argument all cited various infrastructure costs, including installing electrical connections, Internet service, and a facility to protect the TWIC reader as drivers of the increased costs. However, all of these costs are associated with fixed TWIC readers, which are not required by this rule. Isolated facilities without electrical or data connections could use portable electronic readers to comply rather than undertake these measures to install fixed readers. We note that portable electronic readers can be, and are, operated using battery power and wireless communication technology to scan TWICs and check them against the list of cancelled TWICs.

With regard to our preliminary RA, we disagree that the costs of TWIC readers was not applied to barge fleeting facilities. As stated above, as portable electronic readers can be used to conduct electronic TWIC inspections without expensive upgrades to infrastructure, we believe that the price of portable electronic readers estimated in the preliminary RA is applicable to barge fleeting facilities that are not connected to electrical and information infrastructure. Furthermore, barge fleeting facilities were counted in the overall analysis of facilities covered by the proposed rule. Thus, we believe that the preliminary RA sufficiently analyzed the cost impacts for barge fleeting facilities.

Numerous commenters argued that barge fleeting facilities are so isolated they should not be placed in Risk Group A. For example, one commenter recommended that barge fleeting facilities be categorized as Risk Group C, or as an alternative, CDC fleeting areas should be categorized using a risk-based approach based on the geographic location in relation to populations, with those in higher-density locations placed in Risk Group A. One commenter added that for economic reasons, fleets are usually far removed from major industrial or population centers, thus limiting the risk as potential targets for terrorist attacks.

Because of the MSRAM methodology used to determine risk, we disagree that perceived geographic isolation of a particular facility alone should justify lesser security requirements. The risk groupings are based on the averaged MSRAM scores for each class of facility. In conducting our risk analysis, one of the primary factors used was an estimate of the average maximum consequences of a TSI on a class of facility. In MSRAM, the Coast Guard calculates the maximum consequence for each facility, which is the estimate of all damages that would occur from the total loss of a facility caused by a TSI resulting from a terrorist attack. This singular maximum consequence score factors in the total loss of a target, factoring in injury, loss of life, economic and environmental impact, symbolic effect, and national security impact. Further included in the calculation is an estimation of damage done to areas surrounding the facility that would be affected in the event of a TSI, meaning a facility in a densely-populated area could have a much higher maximum consequence score if a TSI would inflict damage on nearby populated areas. Then, the *average* maximum consequence for the class of facilities is derived from the calculations of each facility in the class, taking into account their specific geography. Thus, geographic isolation, or lack thereof, has already been considered in the score calculation. Even considering the geographic isolation of some barge fleeting facilities, this class as a whole presents a risk of a serious TSI, which is why it was included in Risk Group A.

One commenter also argued that because tugboats that service barges are exempt from the requirements for electronic TWIC inspection, due to having fewer than 14 crewmembers, then the barge fleeting facilities should not be subject to TWIC requirements. In the discussion relating to electronic TWIC inspection requirements at facilities that service exempted vessels, we discussed in detail why a facility may be required to conduct electronic TWIC inspection, even if the vessels the facility services are exempted due to low crew counts. This analysis applies equally with regard to barge fleeting facilities.

A variety of other arguments were made to exclude barge fleeting facilities from the electronic TWIC inspection requirements. For example, a commenter argued that barge fleeting facilities by their very nature do not interact with vendors or visitors. We note that TWIC requirements apply to permanent personnel as well as vendors and visitors (some of whom may not have TWICs, and would thus need to be escorted), and that electronic TWIC inspection provides several security enhancements, such as the ability to detect revoked TWICs, that are applicable to personnel as well as vendors and visitors.

Some commenters stated that fleet personnel traffic is very low compared to regular shore maritime facilities and therefore are very low risk. We note that regular personnel traffic is not related to the risk that electronic TWIC inspection is designed to mitigate.

Electronic TWIC inspection helps to ensure that unauthorized personnel are not granted unescorted access to secure areas. This can happen regardless of the number of persons on the facility.

Several commenters argued that screening for personnel on barge fleeting facilities is already in place, and is extensive, including TWIC checks. As stated above, for high-risk facilities, we do not believe that visual TWIC inspections provide enough security. This final rule requires that TWICs be electronically inspected before unescorted access to secure areas of a MTSA-regulated, high-risk facility is

granted. This logic applies to barge fleeting facilities as well as other facilities.

One commenter described a barge fleeting facility as ''one of the few safe places'' for crew transfers. The commenter implied that requiring crewmembers to run their cards through an electronic reader, which the commenter described as redundant and burdensome, could somehow impact safety. Without additional reasoning, we see no linkage between the safety of the crew and the need for security measures, except for the obvious benefits of protecting the crew from a TSI.

Finally, several commenters argued that due to the nature of barge fleeting facilities, TWIC readers would not provide security benefits. One commenter stated that if there is no access from the riverbank to the area where the barges are stored, then the TWIC reader is not adding any security value. Similarly, several commenters noted that while electronic TWIC inspection is required at the access points to each secure area, barge fleeting facilities do not have defined access points, but rather people come in via waterways. Several commenters described barge fleeting facilities as ''parking lots,'' and noted that very few individuals from outside the fleeting facility, other than the crews of tugs, enter the facility. Oftentimes, due to a lack of other means of access, persons entering the facilities need to come via vessel and can do so only with the coordination of the FSO. Lastly, one commenter, while arguing for an exemption for barge fleeting facilities, stated that its barge fleeting facilities have a different risk profile than land-based facilities, noting that the fleeting areas are ''simply unmanned barge parking lots continuously serviced by towing vessels.'' [60]

We have carefully considered the arguments of these commenters, and believe that we can address their concerns through a modification of the regulatory requirement. If a typical maritime facility met the specific criteria that these commenters describe, where there is no bulk CDC at the facility to protect, and no access points at which electronic TWIC inspection would be conducted, the facility would not be considered a Risk Group A facility. We believe that with regard to barge fleeting facilities, the same standard should be applied. For that reason, we are removing the specific reference to barge fleeting facilities in proposed § 105.253(a)(3). Instead, we are adding text, in § 105.110(e), Exemptions, which clearly states that barge fleeting facilities that do not have a secure area are exempt from the requirements in 33 CFR 101.535(b)(1). Based on this change, many of the concerns from the commenters regarding the application and utility of electronic TWIC inspection will be addressed.

We note that simply because the reference to barge fleeting facilities has been deleted from proposed § 105.253(a)(3), some barge fleeting facilities will still be required to comply with electronic TWIC inspection if they meet the requirements of § 105.253(a)(1). Thus, if a barge fleeting facility handles or receives CDC in bulk, it would be considered to be a Risk Group A facility, and would be subject to the electronic TWIC inspection requirements. However, we note that the electronic TWIC inspection requirements would be limited to secure areas only, as towing boats could still service barges without having their crews' TWICs electronically inspected (see the discussion in Section V.C.1, above).

9. Switching Risk Groups

Several commenters requested additional clarification and explanation regarding the NPRM's discussion of moving between Risk Groups. In the NPRM, the Coast Guard stated that it was adding §§ 104.263(d) and 105.253(d) to ''address the movement between risk groups by vessels and facilities, based on the materials they are carrying or handling, or the types of vessels they are receiving at any given time.'' [61] These provisions, which are located at §§ 104.263(b) and 105.253(b) of this final rule, provide flexibility to owners and operators of vessels and facilities that only meet the criteria for Risk Group A classification on an infrequent or periodic basis, such as a facility that only occasionally receives a shipment of bulk CDC. Based on the comments received on this issue, we are finalizing this requirement without change.

One commenter supported the Coast Guard's proposal for movement between Risk Groups noting that the proposal would grant a facility a degree of flexibility to tailor its security precautions to the TSI risks posed at a given time. We appreciate the support.

In the NPRM, we stated that 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 approved security plan, and that the 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 both the higher and lower Risk Groups.

One commenter requested more explicit guidance on the criteria for facilities to move between Risk Groups, asking for guidance regarding the process and for the types of security measures that would need to be in place for a facility to move from a higher Risk Group to a lower one. In response, we note that moving between Risk Groups is not dependent on security measures, it is dependent on whether a facility's change in operations moves it into a different Risk Group. For example, if a facility that periodically handled CDC in bulk were to cease handling that material, it could move from a Risk Group A facility to a non-Risk Group A facility. While such a move is independent of any change in security measures, we note that the facility would still have to amend its FSP with regard to any changes in security procedures.

One commenter stated that his facility occasionally handles bulk CDC for short periods of time. The commenter supported the NPRM's proposal to permit switching Risk Groups, but requested that is should be possible to do so ''without a lot of bureaucratic paperwork.'' In such an instance, an FSP could contain two alternative security arrangements, one for operating as a Risk Group A facility, and one for operating as a non Risk Group A facility, along with the process for switching. Assuming that such an FSP was approved by the COTP, then switching risk groups could be accomplished without additional paperwork each time the operator changes risk groups.

E. Responses to Economic Comments

The Coast Guard received numerous comments from organizations and individuals regarding the costs and benefits associated with the requirement for electronic TWIC inspection. Many commenters, responding to specific requests for information, provided details and opinions regarding the costs of installing and operating an electronic TWIC inspection system. The issues involved the specific costs of purchasing and installing electronic TWIC reading equipment, the operational details concerning electronic TWIC inspection (including how it could increase or decrease the number of persons employed in security positions), and the costs to

[60] USCG–2007–28915–0195, USCG–2007–28915–0213.

[61] 78 FR 17815–6.

transportation workers who may need to replace malfunctioning TWICs. We appreciate these comments and have attempted to integrate them into our RA. We address the specific topics in the sections of this preamble below.

1. Costs of TWIC Readers

We received numerous comments from both suppliers and users of electronic TWIC inspection equipment regarding the standard costs of TWIC inspection equipment. In the NPRM, we estimated the average costs of TWIC readers by researching the equipment costs for all TWIC readers that have passed the TSA's test to conform with its Initial Capability Evaluation (ICE) test, which is maintained and made available to the public by TSA.

One commenter stated that the preliminary RA overestimated the costs of procuring TWIC readers. The commenter stated that the TWIC Pilot Report overstated the costs of TWIC readers, as pilot participants used grant money for incidental security needs, such as PACS, costs related to guard stations, lift gates and fencing. We disagree with the commenter's analysis, and note that we did not use the pilot grants as a basis for the costs of TWIC readers. As stated in the NPRM RA (Section 4.1.1., TWIC reader costs), the costs of TWIC readers were determined using approved TWIC readers that had passed the TSA ICE test.

Multiple commenters stated that the NPRM RA overestimated the cost of TWIC readers, and of the software, needed. One commenter also stated that the Coast Guard used overstated software prices that came from a single supplier and should have used $4,250 for both fixed and portable TWIC readers that included both hardware and software. The commenter added that the price of electronic TWIC inspection continues to fall as technology develops and is deployed on a larger scale. The Coast Guard did not use pricing information from a single supplier, but relied on multiple vendors' publicly available information for regulatory analyses supporting the NPRM and this final rule. While we agree that the price has fallen, we cannot use the prices cited by the commenter directly. However, we note that we have adjusted the TWIC reader cost prices in the final RA. The NPRM RA's TWIC reader cost estimates relied on the ICE List and utilized those equipment costs listed on the U.S. General Services Administration (GSA) price schedule. The QTL includes all TWIC readers that are currently approved by TSA (at the time the final RA was developed) for use in reading TWICs. For the final rule RA, instead of using GSA schedule listed prices for TWIC readers as was the case for the NPRM RA, we utilized the QTL's TWIC reader information to obtain an average cost for portable TWIC readers, and used the GSA schedule for fixed TWIC readers. We note that, for the final rule's cost analysis, we used average TWIC reader prices that we estimated $5,373 for fixed TWIC readers and $7,035 for portable TWIC readers. These prices are close to the one the commenter suggested at $4,250 for either fixed or portable TWIC reader.

The same commenter also added that it would not be necessary to purchase an entirely new PACS software system, and that one could simply add an electronic reader to the existing PACS that supports the perimeter access points for some entities. We agree, and go further in our RA, noting that it is possible to integrate biometric input functions into an existing PACS, rather than install a separate integrated TWIC reader. Use of this discretionary option can reduce electronic TWIC inspection costs substantially, depending on the business operations of the facility using such a system. However, we do not quantify the potential for these cost savings in the RA.

The commenters also made statements regarding the cost for CCL updates, which were echoed by other commenters. They stated that updates to the CCL should be an automated function taking about five seconds, and therefore, these should not be included as an ongoing item with assigned labor expense in the RA. In the NPRM RA, we estimated that the costs to update the CCL would be, on average, 30 minutes per week, which comes to 26 hours per year. In the final analysis, this figure is unchanged. While we recognize that some larger facilities may be able to automate this process, we do not believe that all facilities will have such an automated solution.

One commenter stated that the adoption of the QTL could cause ''change order costs'' to replace more expensive TWIC readers, and that the facilities who need to change TWIC readers should get grants to cover these costs. The Coast Guard disagrees. The final rule will allow many different types of biometric scanners in addition to the ones published on the TSA's QTL, and the rule is not design-prescriptive, so many entities will be able to continue to use existing equipment and therefore should not incur additional costs. The Coast Guard is not mandating that owners or operators use only the TWIC readers listed on the TSA's QTL in this final rule.

2. Number of TWIC Readers at Vessels and Facilities

Additionally, several commenters believed that the Coast Guard has not appropriately addressed the overall numbers of TWIC readers. Several commenters claimed that the NPRM and the RA did not contain accurate estimates of the number of TWIC readers needed for a vessel or a facility. One commenter, who owns multiple vessels and a terminal, estimated that it would need as many as 20 TWIC readers to comply with the proposed regulatory text.

One commenter described the Coast Guard as contradicting itself, by stating in the preamble that Risk Group A vessels would need only one TWIC reader, at the entrance to the vessel, yet the proposed regulatory text required a TWIC reader at ''each entry.'' [62] Another commenter, a city government agency in charge of passenger ferries and terminals, also disagreed with the idea of one point of access per ferry. That agency estimated at least 62 TWIC readers would be necessary for their facilities alone.

We note that the confusion regarding the regulatory text language in the NPRM, which stated that TWIC readers were required ''prior to each entry,'' has been thoroughly discussed above. In this final rule, most vessels are exempted from electronic TWIC inspection requirements, and those subject to them are only required to conduct such an inspection once, prior to entry onto the vessel.

With regard to facilities, we clearly state that electronic TWIC inspection must be conducted prior to each entry into a secure area. Given the nature of facilities, we acknowledge that many facilities will require multiple TWIC readers or other machines capable of conducting electronic TWIC inspection, either because they have a large number of access points to secure areas, or because they have a high throughput of people who must undergo electronic TWIC inspection in a timely manner.

One commenter disagreed with the idea of ''one point of access'' to a ferry, as there may be multiple points of access, and the proposed rule might have required them to install TWIC readers at 62 locations, with additional staffing, to meet the requirements. The Coast Guard disagrees with this assessment. The commenter is not necessarily required to purchase a large

[62] *See* 78 FR 17803 and proposed § 104.265(a)(4), 78 FR 17831.

number of TWIC readers because the electronic TWIC inspection for the vessel crew can be executed on the facility side, rather than at each and every access point to the ferry or the vessel. Given the ''combined security plan'' discussed by this commenter above, it is permissible that a ferry operating a secure facility could have no dedicated TWIC readers, if all crew boarded from secure areas of the facility. Thus, such a ferry operator could comply with the electronic TWIC inspection requirements in this final rule without a wholesale replacement of its security infrastructure with new TWIC Readers.

Several commenters provided qualitative discussions regarding the number of TWIC readers that would be needed at passenger terminals, which while not providing firm numerical information, helped the Coast Guard refine its assessment of how the final rule would affect these sorts of terminals. One commenter argued that the Coast Guard ''does not fully understand the day-to-day operations of Group A passenger vessels and facilities . . .'' and that ''most of these vessels, terminals, and facilities are designated ''public access areas'', with only small areas designated secure, which ''tend to be located away from one another.'' The commenter provided examples of ''a fuel storage area here and a secure communications room elsewhere'' as examples of dispersed secure areas, and stated that ''the everyday reality for a TWIC holder is that he or she is likely to move between secure areas and public areas, as well as between the vessel and facility, multiple times a day in multiple locations.''

Similarly, operators of other passenger terminals made qualitative remarks regarding the number of TWIC readers needed. One commenter, operating a large facility on the West Coast, stated that ''installation of TWIC readers on our vessels and at our terminal would provide a negligible improvement in security, which would come at an unreasonable cost given that WSF has already implemented a superior security infrastructure.'' We note that, at the time the comment was made, the NPRM had not proposed the option that would allow the operators of facilities to integrate electronic TWIC inspection into their PACS. Given comments like these, we expect that larger passenger facilities that have already implemented PACS would be likely to use that option rather than installing TWIC readers in a parallel security structure.

Commenters representing smaller facilities also provided qualitative information. One commenter stated that ''our terminals are a mix of secure and public areas where employees move between areas throughout the day,'' indicating that TWIC readers would be needed at multiple access points, not just at the entrances to the facility. Similarly, a facility operator in San Diego noted that ''careful consideration needs to be taken into account for the passenger vessel industry because our vessels and facilities are not just one big secure area, but rather are interspersed amongst public areas.''

Based on the substantial numbers of comments regarding the implementation of electronic TWIC inspection at passenger facilities, as well as the policy changes in this final rule, we have re-evaluated how we analyzed the costs of this rule for passenger facilities. In the TWIC pilot program, TWIC readers were typically only employed at the exterior access points to facilities, whereas in the final rule things are quite different. For passenger facilities, it is likely that electronic TWIC inspections would not likely take place at the main entrances where passengers enter and exit, as those areas would lead to ''passenger access areas'' which are, by definition, not secure areas and do not need to be controlled by a TWIC reader. Instead, TWIC readers or a PACS would likely be installed throughout the facility, at each entrance into a secure area, to ensure that only TWIC-holders had access to these secure areas of the facility.

Furthermore, based on the comments, we are reasonably certain that the largest passenger facilities are much more likely to implement the electronic TWIC inspection requirement by adding a biometric input method into their PACS, rather than by developing an entirely parallel TWIC reader system. This option permit substantial cost savings and operational efficiency benefits for facilities that have already invested in, as one commenter stated, ''superior security.''

For these reasons, we have adjusted the ''number of TWIC readers'' used by passenger facilities as the cost basis in our analysis. For the largest 5% of facilities, we have assumed a larger number of TWIC readers, representing our estimates that these facilities are quite extensive and will require either modification of their PACS or installation of a substantial TWIC reader system. For other passenger facilities, we have left the estimate at 2 access points per facility, for a total of four readers. We estimate that these facilities would likely have an access point to the vessel, as well as an additional access point to secure areas of the facility, such as a storage room or communications area. We develop this reasoning at more length in the accompanying regulatory analysis.

One commenter, operating several large terminals on the West Coast, provided information on the maintenance of readers. The comment estimated that they are planning to pre-purchase 74 contact card reader inserts for their 33 existing readers over the next three years at a total cost of $28,800, or approximately $300 per reader per year. We have used this information to increase our cost estimate for the maintenance of readers from 5 percent of the cost of a reader to 10 percent of the cost of a reader per year to cover the expense of insert replacements.

With regards to the number of TWIC readers, Coast Guard recognizes that there may be variability in the number of electronic readers required for any specific facility or vessel due to a large range of facility sizes, configurations, PACS types, and throughputs that will necessitate large variations in the numbers and types of TWIC access points. For the purposes of producing a cost estimate in the NPRM and RA, Coast Guard used data from Facility Security Plans (FSPs) to estimate the number of access points per facility and the TWIC pilot data to estimate an average number of TWIC readers needed per access point for a vessel or facility. The average number of TWIC readers at a vessel or facility was derived from the actual number of TWIC readers installed per facility or vessel in the pilot study that ranged from between 1 and 39 TWIC readers based on a minimum number of 1 to 24 access points from the FSPs. While we appreciate specific information about individual facilities, we note that the average figures developed through the TWIC Pilot Program, which sampled a broader spectrum of facilities, provides the best data for average numbers of TWIC readers and access points.

3. Transaction Times

Many commenters stated that conducting electronic TWIC inspection at each entry to a secure area on a day-to-day basis would negatively impact the time needed to make entries. These commenters did not, however, provide any specific information regarding transaction times. One commenter that operates a cruise ship terminal stated that conducting electronic TWIC inspection with a biometric identification component takes 20 to 30 seconds per transaction, and thus would result in intolerable delays, especially regarding baggage handlers who enter secure areas repeatedly (we would note

that the RUA provisions in this final rule may offer flexibilities to mitigate transaction time concerns).

One commenter provided feedback on its TWIC reader experience. According to this commenter, the learning curve for adopting TWIC readers is short, with the proper signage and instruction. Within one year of implementing TWIC readers into the facility, the commenter had over 1 million reads that take 4 seconds each, and the use of TWIC readers on inbound trucking has caused no delays. Further, the commenter suggested that TWICs can last 3 years without breakage or delamination issues if properly cared for, and believes that many TWICs were broken because the issue of their care was not communicated. The Coast Guard agrees with some of the points made by this commenter: The learning curve for using TWIC readers is relatively short and TWIC readers can handle a large volume of reads. However, the read time may not be 4 seconds on average across all the TWIC reader users, although we appreciate the data point supplied by the commenter.

Other commenters also felt that the Coast Guard overestimated transaction times and the amount of time needed for a CCL update. With regard to the CCL update, we estimated that it would take 0.5 hours to update the CCL. One commenter suggested that the process could be automated. We agree that some operators could automate the process, but currently, we are unaware of any that do. We still believe that absent automation, our estimate of time is accurate.

Transactions were discussed by an additional commenter. One commenter stated that he had heard from an operator who has conducted over 1 million electronic TWIC transactions, and who had experienced an average transaction time of 3.5 seconds, as opposed to the 8 seconds per successful transaction experienced during the TWIC Pilot Program.

In response to comments regarding transaction times, we acknowledge that transaction times may vary based on equipment, software, environmental conditions, user familiarity, the condition of the TWIC, and perhaps many other conditions. This variability is reflected in the range of transaction times spanning from 3.5 to 30 seconds provided in the comments. The TWIC pilot collected data from a variety of facilities and circumstances, and produced an overall average of 8 seconds per transaction. We note that the range of times collected by the Pilot Program (which used TWIC readers from the ICE list) was from 6 to 27 seconds per transaction, which is not inconsistent with the experiences of the commenters.[63]

One commenter stated that the 17.1 percent failure rate from the TWIC Pilot Report is a high figure to use in the regulatory impact analysis, since the primary cause of TWIC read failures (internal antenna failures) was addressed by the design of better cards. The commenter noted that these older cards have been retired since 2009. While we believe that the design of TWICs themselves has improved, without comprehensive data demonstrating that improvement, we continue to use the 17.1 percent failure rate from the Pilot Report in our analysis as the best available estimate. This failure rate is still a reasonable one to use when estimating the delays due to TWIC reads because there are other reasons for TWIC reads to fail, such as exposure to harsh weather. Finally, we note that even this higher failure rate did not produce measureable throughput delays, and thus a lower failure rate would not substantially affect the transaction costs of this rule.

One commenter argued that between 2,500 and 3,000 people a day undergoing visual TWIC inspections would cost a great deal of money, and asked if they could use a PACS instead. Certainly nothing in this final rule precludes voluntary compliance with the requirements for electronic TWIC inspections, and the Coast Guard encourages owners and operators to go beyond minimum levels of compliance. The Coast Guard believes that this final rule will not only increase security but may also reduce the costs for owners and operators who are currently relying on visual TWIC inspection. The final rule also allows other, less expensive biometric scanners to be integrated with existing facilities' PACS, as long as a biometric TWIC read is accomplished.

4. Security Personnel

We received several comments regarding potential reductions in security personnel that could result from the mandatory use of electronic TWIC inspection. These comments generally fell into two categories. Some commenters felt that the requirements in the proposed rule, if finalized, would cause employers to reduce security staff, as fewer guards would be needed to conduct visual TWIC inspections. While some commenters believed this reduction would be a detriment to overall port security, in contrast, other commenters stated a possible reduction in personnel costs is a benefit we did not consider in the NPRM RA. We do not believe that this final rule will have a substantial effect on staffing for several reasons.

With regard to the argument that use of electronic TWIC inspection would lead to a reduction of security, we believe this results from a misunderstanding of the role of inspection and the role of security personnel. While electronic TWIC inspection can be used as a substitute for visual TWIC inspection, the role of a security guard goes far beyond this limited function, including providing other components of access control and physical security. If anything, we believe that electronic TWIC inspection can improve the capability of security personnel by allowing them to focus on their more specialized security-providing roles.

One of the reasons suggested for a reduction in staffing related to a scenario in which a vessel's crew slightly exceeded the threshold limit for an exemption from the electronic TWIC inspection requirement, and the operator of the vessel decided to reduce the crew size in order to qualify for the exemption. By clarifying that the number of crew used to determine whether the vessel is exempt is based on the minimum manning requirement in the COI, we believe that this scenario will not come to pass. Unlike a situation in which a vessel operator could dismiss an optional deckhand to qualify for the exemption, it is exceedingly difficult, if not impossible, to alter the minimum manning requirements of the vessel. Alternatively, some commenters believed that by installing TWIC readers, operators of facilities could dismiss security guards. We are not aware of any instances of operators terminating security personnel as a result of installing TWIC readers (which should have been reflected in a change to a security plan and approval by the local COTP). We also note that pursuant to PAC–D 01–11, facilities are already permitted to employ TWIC readers in lieu of visual TWIC inspection on a voluntary basis.

Some commenters felt that the proposed requirements, especially for those vessels and facilities not in Risk Group A, would increase the necessary number of security guards per shift. These comments were based on the erroneous assumptions about the use of electronic TWIC inspection with regard to vessels, as well as the mischaracterization of the requirements for electronic TWIC inspection with regard to vessels and facilities not in

[63] See Pilot report, located in the online docket for this rulemaking at USCG–2007–28915–0121, Appendix G, pp. 49–50.

Risk Group A. We believe that the clarifications in this final rule clearly illustrate that the scenarios in which large numbers of security personnel are required on board vessels will not apply. Furthermore, access control requirements for vessels and facilities not in Risk Group A are unaffected by this final rule.

5. Other Cost Comments

Several commenters stated that the NPRM requirements were expensive. For example, one commenter stated that the expense of outfitting their vessels and facilities with TWIC readers would be enormously expensive compared to their normal operating budgets. In this particular instance, the Coast Guard notes that vessels owned by this commenter are not in Risk Group A and are not subject to the requirements in the final rule for TWIC readers. Most of these commenters did not include estimates or specific costs to support their claims. For the one commenter that provided a specific cost estimate, we incorporated the information to increase our estimate of the cost to maintain readers. The Coast Guard has carefully considered this input on burden and in this final rule has further reduced burden from the NPRM and ANPRM. See the final RA, included in the docket for this rulemaking, for the Coast Guard's analysis of the available data.

One commenter suggested that the NPRM did not appear to consider the secondary economic cost impact that would result from the disruption of such facilities from a TSI. The same commenter also stated that the break-even analysis in the NPRM did not consider the economic cost impact that would result from an attack on a petroleum facility. This latter statement is correct, because petroleum facilities are not included in the affected population of this rule. Furthermore, the former statement is correct, although the net effect of adding additional categories of terrorism impacts not now quantified in this rule would be to increase the benefits of avoiding a TSI.

Multiple commenters stated that the NPRM did not do a cost analysis of domestic inbound fleeting areas (also known as barge fleeting facilities), and that it did not fully evaluate the impact of TWIC readers on those fleets. More specifically, one of these commenters felt that owners of those fleets would have to make a significant monetary investment to install equipment in an area that might not be able to support it.

The NPRM did include all those affected domestic inbound fleeting areas in the cost analysis. It fully assessed the impact on an average facility, including the barge fleeting facilities. However, this final rule no longer specifically requires barge fleeting facilities to install TWIC reader equipment (see Section V.D.7 of this preamble), which addresses the concerns of these commenters.

One commenter said that it should not take 25 hours to update a facility security plan for TWIC. The Coast Guard disagrees. For some facilities, it may take fewer hours, but for many others it will take more than 25 hours, especially if changes to security plans are reviewed by multiple people, and we believe that the 25-hour assumption is a reasonable average for the full range of vessels and facilities impacted by this rule.

One commenter suggested that the TWIC is not designed to be handled multiple times per day, (the commenter suggested that at their passenger ferry facility, an average employee could expect to have their TWIC inspected 2,400 times per year) and therefore this rule would likely cause TWICs to degrade and malfunction at a high rate, leading to increased costs for mariners to replace degraded TWIC cards. We disagree with this analysis for two reasons. First, while some older TWICs were issued with antennas that proved unreliable, the cardstock was upgraded in 2009 to be more reliable and can be used frequently without degrading. Second, we note that at most large facilities, such as the passenger facility at issue, employees use a PACS for access control rather than the physical TWIC. This final rule permits the use of a PACS card for access control in lieu of the TWIC, so we expect that the many employees at larger facilities will not suffer any degradation of their TWICs during normal usage.

6. Costs Exceeding Benefits, Cost-Effectiveness, and Risk Reduction

Many commenters expressed a concern that the costs of installing TWIC readers on their vessels and facilities would exceed their benefits. One of these commenters said it has already implemented a superior security infrastructure and the installation of TWIC readers would be duplicative of security measures already in place. Another of these commenters expressed the view that terminal facility TWIC readers would be an unnecessary burden and cannot be justified for their operations. Another commenter felt that the added burden of the TWIC readers does not enhance overall security for their nature of operations. In addition to these commenters who questioned whether the costs of the TWIC reader rulemaking exceed the benefits, several others argued that the TWIC card readers would neither significantly enhance security on U.S. facilities and vessels, nor make our nation safer.

The Coast Guard disagrees. The regulatory impact analysis we provide in the docket discusses at length why and how security will be enhanced by this rule. The commenters do not appear to account for the benefits to the nation and its economy of avoiding TSIs or that this rule is a Congressional mandate, and therefore, it addresses a market failure in which individual owners and operators tend to under-invest in security infrastructure, equipment and operations. As previously explained, we used a risk-based approach to apply these regulatory requirements to less than 5 percent of the MTSA-regulated population, which represents approximately 80 percent of the potential consequences of a TSI. The provisions in this final rule target the highest risk entities while minimizing the overall burden of the rule. We conducted a robust alternatives analysis that considered the ''break-even'' point of several different alternatives and we chose the alternative that shows the final rule will be cost effective if it prevents 1 TSI with every 234.3 years. Such small changes in risk reduction strongly suggest the potential benefits of the proposed rule justify its costs.

One commenter argued that reduction of human error, as part of visual TWIC inspection, should be a quantified benefit of the final rule, and not an ''unquantifiable'' benefit as described in the preliminary RA. However, the commenter did not ascribe a dollar value to this benefit that could be quantified. Considering the RA did not attempt to quantify each individual security threat mitigated, but instead provided an overall break-even analysis that encompassed the rule, we believe our analysis remains appropriate for this issue.

7. Cumulative Costs of Security-Related Rulemakings

Some commenters warned of the cumulative economic impacts of this rulemaking with several other finalized rules across Federal agencies. These comments did not provide specific data or information on these cumulative economic impacts. Understanding and considering the concerns about these cumulative economic impacts of all maritime security regulations, the Coast Guard decided to apply the final rule to a smaller population of MTSA-regulated entities after conducting its regulatory impact analysis. The Coast Guard

believes that the increased flexibility of the final rule compared to the proposed regulations will help lower costs and ease the burden on the regulated stakeholders.

8. Small Business Impact

One commenter expressed concern that its small profit margin would be negatively affected by new expenses for security due to changes to technology and additional regulations. Cognizant of regulatory impacts on small businesses, the Coast Guard sought to minimize these impacts by allowing businesses to integrate TWIC readers into their existing PACS, and to choose from a variety of biometric scanners that may cost less than those approved by the TSA and listed on the TSA's QTL.

*F. Other Issues*

1. The GAO Report and the TWIC Pilot Program

Several commenters noted concerns with the final rule in light of the May 2013 GAO report ''Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed'' (GAO–13–198). Two commenters specifically called attention to the GAO report's suggestion that results were less reliable due to ineffective evaluation design and the lack of requisite data. The Coast Guard fundamentally disagrees with the statement. Although there were many challenges in the implementation of the TWIC reader pilot, considerable data were obtained in sufficient quantity and quality to support the general findings and conclusions of the TWIC reader Pilot Report. The pilot obtained sufficient data to evaluate TWIC reader performance and assess the impact of using TWIC readers at maritime facilities. Furthermore, the Coast Guard supplemented the information from the TWIC Pilot Program with other sources of information. For example, in the RA, the Coast Guard estimated the number of access points per facility by facility type through the use of an independent data source (Facility Security Plans), and estimated the costs of TWIC readers through published pricing information. This independent data supplemented what we learned through the pilot and helped account for TWIC reader implementation at all access points when developing the NPRM.

Similarly, multiple commenters suggested that the Coast Guard should not move forward on this final rule due to the GAO recommendations. We would encourage those who criticize the TWIC Pilot Program to closely review how the information gained in the program was used in the development of this rulemaking. Because of the testing conditions endemic to a voluntary pilot program, the TWIC Pilot Program encountered many challenges. The Coast Guard was aware of the pilot's limitations, and used it with discretion in developing the NPRM and, subsequently, in developing this final rule. For that reason, the pilot results were not the sole basis for the NPRM. The Coast Guard believes that the pilot produced valuable information concerning the environmental, operational, and fiscal impacts of the use of TWIC readers. The Coast Guard believes that data were obtained in sufficient quantity and quality to support the general findings and conclusions of the Pilot Report. The pilot data informed aspects of the rulemaking in which no other data were available. The Coast Guard is convinced that TWIC, including the use of biometric readers, can and should be a part of the nation's maritime security system, for the reasons cited extensively in this final rule.

Two commenters suggested that individual TWIC Pilot Program participants were not provided the opportunity to review the final draft Pilot Report prior to publication. In response, the Coast Guard participated along with TSA and the independent test agent in individual close-out meetings with each of the pilot participants. Individual test phase reports were provided to participants in advance of those meetings to verify and answer questions and concerns.

One commenter suggested that they heard from participants that information contained in the Pilot Report was inconsistent with the participants' records. We note that this commenter was not a pilot participant, nor did we receive such feedback from pilot participants. Given the nature of the program, we believe that the information from the pilot was generally helpful in providing data relating to certain operational aspects of the TWIC program.

The RA for this final rule accounts for maintenance, replacement, and operation costs of TWIC readers in addition to the costs reported in the Pilot Report, contrary to the GAO's assertions. As both the Pilot Report and the GAO's review note, not all facilities implemented TWIC readers at all access points during the pilot in the same way they may have to do in the future to meet the requirements of this final rule. We believe that the immaturity of TWIC reader technology at the onset of the pilot, the voluntary nature of the Pilot Program, and lack of full cooperation at all facilities were major contributors to the pilot's limitations. Furthermore, we note that the additional flexibility afforded by this final rule, especially with regard to utilizing PACS as a means to undertake electronic TWIC inspection, will further reduce the negative operational impacts of the TWIC requirement that were experienced by some participants during the pilot.

One commenter took the opposite position, arguing that the GAO report went beyond the required purpose of assessing the validity of the pilot, and that TWIC reader technology could be seamlessly integrated into their facility access control systems. While we do acknowledge that there were some problems with the pilot, overall we agree with the commenter that it demonstrated the ability to integrate TWIC into access control systems at a wide range of maritime facilities.

One commenter suggested that the Coast Guard does not have an accurate accounting of how long it will take to resolve TWIC reader issues. We addressed a similar comment in the section of this preamble regarding malfunctioning access control systems. Per that discussion, we note that in this final rule, we are removing the specific time period for repairs, and that restoration of an access control system will be handled in accordance with the procedures for the reporting requirements for non-compliance as described in 33 CFR 104.125, 105.125, and 106.125. These sections require the owner or operator to notify the cognizant COTP, and to either suspend operations or request and receive permission from the COTP to continue operating.

Additionally, one commenter stated that the NPRM did not address the error rate experienced during the Pilot Program which, with repetitive failure, created distraction, confusion, and complacency with an overall degradation of security. The commenter suggested that another pilot should have been conducted to validate the original findings given technology problems encountered. The Coast Guard disagrees. The RA section in the NPRM did address error rates as potential opportunity costs associated with delays as a result of TWIC reader requirements. Furthermore, the Pilot Report did acknowledge both TWIC reader errors and card failures as challenges that were faced. The Coast Guard believes that the combination of technology advancement since the Pilot Program started and the enhanced flexibility and the movement to a more performance-based standard

in this final rule will have a significant role in reducing the rate of TWIC reader failure and the overall effect of TWIC reader failure on a vessel or facility. As noted in the NPRM, the Coast Guard anticipates that the rate of card failure requiring replacement will decrease as TWIC reader use increases. We believe the number of unreadable TWICs initially identified will decrease as the increased use of TWIC readers will enhance TWIC validity and readability by identifying damaged TWICs. However, as with any such critical system and as we have noted in previous sections, it is important for operators of vessels and facilities affected by this final rule to adequately address potential electronic reader failure scenarios in the development of their security plans to ensure that measures are identified, and to seamlessly react to a single electronic reader failure or, in the worst case, an entire PACS failure in a way that continues to meet the security intent of this rulemaking. Please see discussion in section V.B.3.d on malfunctioning access control systems for more discussion on this subject.

One commenter highlighted GAO's assertion that DHS has not yet adequately demonstrated how the TWIC actually enhances maritime security. We have addressed the efficacy of the TWIC program as a whole in Section V.A of this preamble.

One commenter stated that the GAO report failed to account for the opinions of various container terminal operators that participated in the Pilot Program, and suggested that the GAO report itself was flawed and went beyond its mandate. The Coast Guard appreciates the extremely valuable information provided by all vessel and facility operators during the course of this rulemaking, and has evaluated all comments in comparison with economic and environmental data to enhance this final rule to address the greatest security threats in which TWIC and TWIC readers provide utility in the prevention of a TSI. We have modified this final rule in a manner that allows for the greatest flexibility for non-Risk Group A vessel and facility operators to implement electronic TWIC inspection procedures on a voluntary basis. Additionally, the Coast Guard is committed to the continued security of the nation's ports. Accordingly, we will continue to evaluate the need for TWIC readers on vessels or facilities not covered in this final rule, and, should future cost benefit analysis show increased TWIC reader cost-effectiveness to address the threats to vessels and facilities within our ports, we may propose further requirements.

Several commenters suggested that the Coast Guard did not engage with industry groups and advisory committees, other than TSAC, when drafting this rulemaking. The Coast Guard took into consideration input from a wide range of industry representatives during the development of this final rule through both formal and informal interaction. Formal interaction with stakeholders occurred in the form of direct contact with the National Maritime Security Advisory Committee, interaction with TWIC Pilot Program participants, and during multiple port and facility visits aimed at gathering specific feedback from industry on TWIC and the use of TWIC readers. Informal interaction occurred through multiple TWIC information sessions at industry-sponsored events such as meetings and conferences, and through feedback in the form of comments to both the ANPRM and NPRM for this rulemaking.

2. Additional Comments

a. General Comments on the TWIC Program

Many commenters supported the Coast Guard's implementation of a delayed effective date for this final rule. As stated in the **DATES** section above, the Coast Guard will delay the effective date of this rulemaking by 2 years to allow the regulated industries time to comply with this final rule. One commenter asked if a non-Risk Group A vessel or facility decided, 1 year from the date of publication, to move up to Risk Group A, how many years that entity would have to comply with this final rule. In this example, the entity would have 1 more year to comply with the electronic TWIC inspection requirements of this final rule. All vessels and facilities meeting the Risk Group A criteria after the effective date of this final rule will have no extra time to comply, as the regulation will be in force. The commenter also asked what procedures such a facility would have to follow. Such a facility would have to adjust its FSP in accordance with all applicable regulations, and then implement the requirements of the approved FSP.

Some commenters expressed concerns about the durability and reliability of TWICs themselves. As revealed in the TWIC Pilot Program, many users experienced problems with the TWIC. We note, as multiple commenters did, that prior to 2009, some cards were issued with antennas that experienced high rates of failure, but given the 5-year expiration period of the TWIC, those cards should all be replaced by the time this final rule is effective. Furthermore, due to the flexibility added by this final rule, should an environment prove to have a negative effect on the TWIC, owners and operators can use one of the alternative means described above to provide for access control while keeping TWICs in a secure location where they will not become damaged.

One commenter stated that mariners are already subject to background checks, which should preclude the need for another check conducted by an electronic reader. We would note that the electronic TWIC inspection does not actually conduct an additional background check, but merely verifies the individual presenting the card is the same person who underwent the original background check. This commenter also suggested that random Coast Guard checks of the TWIC ensure adequate security. We disagree, and believe that security validation at high-risk vessels and facilities should be conducted thoroughly, not occasionally, for the reasons described in this rule.

One commenter in a public meeting suggested that because of the TWIC program, driver's licenses and other forms of identification are no longer allowed for access to facilities, in favor of a TWIC, and that this has reduced security. The Coast Guard disagrees, and believes that TWIC enhances security. We note, for example, that merely having a driver's license does not indicate that an individual has passed a background check.

Some commenters discussed both possible TSIs and terrorist attacks which would not, in their view, have been averted by a TWIC reader requirement. The Coast Guard notes that the electronic TWIC inspection requirements are only part of the Coast Guard's comprehensive port security program and will not address all attack scenarios. Issues relating to the overall effectiveness of the electronic TWIC inspection programs are discussed in Section V.A, above.

Some commenters supported the use of the TWIC as a single Federal credential, and suggested that it should preempt and supersede other State, local, or site-specific credentials. One commenter suggested that using the TWIC as the only credential a person would need to enter multiple secure facilities would have substantial economic benefits, especially for individuals such as truck or bus drivers that need to access many different secure facilities. These benefits, according to the commenter, would include conducting only a single background check (as opposed to

multiple background checks that might be needed to obtain State, local, and site-specific credentials), as well as reduced ''wait time'' as security credentials are examined.

While there is an efficiency argument to having a single, nationwide credential, we believe that the disbenefits of such a mandatory program are substantial and outweigh that efficiency. To start, we note that part of the increased flexibility of this final rule allows for alternative cards, such as employee ID cards, to achieve electronic TWIC inspection, provided that these cards are linked to a TWIC in a manner described above. As several commenters noted, possession of an authorized TWIC should not, in and of itself, grant the TWIC-holder access to any secure area on any vessel or facility. While a valid TWIC is a necessary component for unescorted access to secure areas, it will not be the sole reason, as owners and operators must exercise their right and responsibility to decide to whom to provide such access.

One commenter expressed concern regarding the tiered approach for the use of TWIC readers. This commenter suggested that multiple access control procedures could result in confusion for persons who visit many different facilities. The commenter proposed that the Coast Guard require the installation of TWIC readers at Risk Group A and B facilities, and require that Risk Group C facilities maintain portable TWIC Readers. We acknowledge that using different access procedures at different facilities could be confusing. Furthermore, for the reasons discussed extensively, we do not believe that requiring electronic TWIC inspection at non-Risk Group A facilities is an effective use of resources at this time.

Two commenters suggested an alternative process where inspection requirements are relaxed during peak hours. One commenter stated that between 7 a.m. and 9 a.m., hundreds of vehicles enter a particular facility, often with multiple passengers, and that requiring biometric identification of each passenger could result in traffic delays. The commenter suggested that only the driver should be required to undergo electronic TWIC inspection, while the passengers could present their TWICs for visual TWIC inspection. The Coast Guard does not agree with this approach, as it creates a fairly obvious and exploitable gap in security.

While we have worked to increase operator flexibility to reduce delays and minimize their effects, we have estimated in the Coast Guard's RA that some facilities may have to make modifications to business operations to accommodate electronic TWIC inspection requirements, such as increasing the number of access points for vehicles. Furthermore, it may be possible at some facilities to conduct electronic TWIC inspections at locations employees would walk through after disembarking from their automobiles.

Several commenters considered existing requirements under the MTSA and/or under the International Ship and Port Security Code to be sufficient for themselves and others, and that electronic TWIC inspection requirements should not apply to them. We believe, for reasons extensively detailed in this document, that the statutorily-mandated enhancements to access control in this final rule have been applied to the class of vessels and facilities to which they are most cost-beneficial.

One commenter was concerned at the prospect of TWIC readers being considered ''no-sail equipment,'' that is, equipment which must be operational before a vessel can leave. We note that while a situation where a TWIC reader could become no-sail equipment theoretically exists (for example, if there were only one TWIC reader available on the vessel, no TWIC readers at the facility, and no portable TWIC readers available), we have elaborated on the many ways in which this could be avoided through advance planning. This final rule elaborates on procedures which would be acceptable in the event of an electronic reader or system failure. We would recommend that operators of vessels or facilities required to undertake electronic TWIC inspections utilize robust systems that are capable of withstanding a single point of failure.

One commenter expressed confusion as to how the electronic TWIC inspection requirement would apply to the aviation industry. We note that the requirement for electronic TWIC inspection at Risk Group A vessels and facilities applies equally to individuals entering via helicopters or other airborne means. In such an instance, it would be the responsibility of the owner or operator to conduct electronic TWIC inspections to ensure that all persons granted unescorted access to secure areas within the facility or upon boarding the vessel possess a valid TWIC.

One commenter in a public meeting suggested that multiple entrances and departures in a day may pose a safety risk, if for example a facility is surrounded by public roads and highways. We believe that businesses can design their access points to secure areas in such a way that mitigates traffic impacts and potential safety concerns regarding public roads. We note that with the requirement for electronic TWIC inspection prior to each entry into a secure area of the facility, the security risk of such an environment would be greatly mitigated compared to a system that only required, for example, one inspection per day.

One commenter requested that the TWIC be used as a universal identification card for entrance to transportation facilities, replacing the issuance of State, county, and facility-specific credentials. The commenter also suggested that bus and motorcoach drivers should be eligible for TWICs. Noting that many drivers travel to numerous MTSA-regulated sites, the commenter argued that using the TWIC exclusively could significantly reduce the costs and other burden associated with the need for multiple security credentials. While we do not dispute the efficiency argument, we are not requiring the use of a TWIC as universal identification card for a number of reasons. First, again, this suggestion is out of scope of the rulemaking, which is limited to the requirement for electronic TWIC inspections. Moreover, we note that nearly all MTSA-regulated facilities restrict access not only to those who have a TWIC, but also to those who have a valid reason to be on the premises. As many commenters repeated, simply having a TWIC does not guarantee access to a secure area of a vessel or facility. Many vessels and facilities use employment-specific identification cards both as a means to ensure that a person has been vetted as well as a means to show that they are employees. Furthermore, some of these PACS cards are used to track employee locations or restrict access within the facility. Requiring all facilities to use the TWIC exclusively could negatively impact security and business operations by removing the benefits of facility-specific access cards.

Several commenters encouraged the Coast Guard to dismiss or devalue the comments from other commenters. In accordance with the Administrative Procedure Act, the Coast Guard considered every comment it received, both through the docket and through public meetings, before issuing this final rule.

Several commenters made statements asserting that their operations were more secure or employees better trained than public transit operations and employees, and yet the latter may not be required to perform electronic TWIC inspections. While we cannot attest to the validity of these statements, we continue to believe that the improved security of electronic TWIC inspection,

compared to visual TWIC inspection, is warranted for high-risk vessels and facilities for the reasons discussed extensively in this preamble.

One commenter believed that disbanding the TWIC program would remove the ''false crutch that TWIC provides'' and encourage greater operational security. For the reasons discussed above, we disagree and believe that TWIC provides a necessary and effective element of a comprehensive security system.

b. Clarification of Specific Items

Several commenters asked for clarification about a term or idea used in the NPRM, or asked the Coast Guard to define it outright. Explanations of various terms are described below.

One commenter requested clarification of the term ''each entry.'' As stated above, with regard to facilities, ''each entry'' is each distinct transition from a non-secure area to a secure area. With regard to vessels, ''each entry'' is each distinct transition from a non-secure area prior to boarding the vessel.

One commenter asked about the definition of ''escorting,'' specifically whether a visual inspection, such as the use of closed-circuit television (CCTV) systems, would be an acceptable form of escorting. In response, we refer the commenter to the detailed guidance on escorting found in NVIC 03–07. There, we provide guidance and examples of circumstances in which the use of surveillance equipment, including CCTV systems, might be sufficient for escorting purposes. The specific facts and circumstances of each case will determine whether the Coast Guard will permit CCTV systems for such purposes. In general, escorting in restricted areas requires side-by-side accompaniment with a TWIC-holder. However, escorting in secure areas that are not also designated restricted areas does not always require side-by-side accompaniment. In such secure, non-restricted areas, escorting may be sufficient through CCTV or other monitoring method (*see* 33 CFR 104.285 and 105.275). Where such monitoring is appropriate, the general principle applies that monitoring must enable sufficient observation of the individual with a means to respond if the individual is observed to be engaging in unauthorized activities or crossing into an unauthorized area.

One commenter raised the issue of how railroads would interact with the new electronic TWIC inspection requirements. PAC 05–08, ''TWIC Requirements and Rail Access into Secure Areas,'' is the existing policy guidance regarding railroad access as it relates to facilities in the TWIC program. This guidance allows the railroad company's local or regional scheduling coordinator to provide information on the TWIC status of the crew, and if all crewmembers are valid TWIC-holders, allows them to enter the secure area of a MTSA-regulated facility without further inspection of their TWICs. PAC 05–08 also permits trains on ''continuous passage'' through a facility to proceed without stopping to check TWICs in certain circumstances. One commenter, representing railroad companies, stated ''[n]either the need for, nor the advisability of, a change has been demonstrated'' in regards to this guidance. We agree, and reaffirm the guidance in PAC 05–08 in this final rule, with one caveat. If PAC 05–08 would require that an individual's TWIC be checked at a Risk Group A facility, it must be checked using electronic TWIC inspection.

c. Comments Outside the Scope of This Rulemaking

Many commenters provided comments beyond the scope of this rulemaking when discussing the TWIC program generally. In addition to concerns about card stock and card reliability, comments concerning applicability of the TWIC card to other U.S. government or government-regulated facilities, TWIC card applications, delays in issuing or renewing TWIC cards, and those concerning TWIC card waivers are all beyond the scope of this rulemaking. Similarly, it is beyond the scope of this rulemaking to require biometrics in the U.S. Merchant Mariners Document, commonly known as a ''Z-Card,'' or for multiple mariner documents to be consolidated into an ''all-in-one'' credential. The scope of this rulemaking is to establish requirements for electronic TWIC inspections on vessels and facilities regulated under the MTSA.

Several commenters suggested ideas about how TSA's CCL could be improved or altered. We note that these ideas are outside the scope of this rulemaking and are best addressed to the TSA.

Some commenters expressed concerns with the background check criteria for receiving a TWIC. For example, one commenter noted that certain longshore workers were erroneously denied a TWIC based on incorrect information in the Federal Bureau of Investigation database, and another experienced difficulty proving citizenship because he was born on a military base. While we are aware that some challenges exist in the enrollment and application process, we believe that the vast majority of enrollments are conducted accurately and efficiently, and that problems are generally dealt with in a courteous and timely manner. We note, however, that concerns relating to the background check are outside the scope of this rulemaking.

One commenter expressed concern that no regulatory analysis was done for workers who need to acquire and pay for a TWIC. Another commenter stated that for workers in remote areas, the cost of obtaining a TWIC can be higher due to travel costs. We note that this final rule does not require any additional individuals to acquire a TWIC, and thus the comment is outside the scope of this rulemaking. However, we would refer interested parties to the RA for the TWIC final rule, available at *http://www.regulations.gov,* docket number TSA–2006–24191–0745, for a detailed analysis of these costs.

One commenter expressed concern that there is no requirement in this rule that obligates an employer to report individual TWIC-holders to the Coast Guard who commit TWIC-disqualifying offenses. This issue is outside the scope of this rulemaking.

One commenter criticized facility owners for poor quality fences despite receiving money from the Federal government to improve security. This commenter also suggested that instead of investing funds into the TWIC readers, the Coast Guard should spend the money on bettering terminals and their surrounding areas. These comments do not address the use of electronic TWIC inspection, and therefore, are out of this rule's scope.

One commenter in a public meeting described a system where ''personnel from other companies'' must, prior to arrival at his facility, fax his company with basic information including whether or not the visitor holds a TWIC. Facility procedures other than those relating to the electronic TWIC inspection procedures are beyond the scope of this rulemaking.

One commenter recommended using closed-circuit television systems for purposes of visual inspection, rather than having a guard physically present. This rule relates to electronic TWIC inspection, and we do not believe it is within the scope of this rulemaking to issue guidance on proper visual identification procedures.

One commenter suggested that, if not requiring electronic TWIC inspection for all Risk Groups, the Coast Guard should institute a ''display and challenge'' requirement for all secure areas. This would require that all persons with unescorted access display their TWIC or

other credential when in a secure area. As this final rule only relates to electronic TWIC inspection, such a suggestion is out of scope of this rulemaking.

One commenter suggested that the Coast Guard has been lax in pursuing administrative action for TWIC-related offenses, such as loaning TWICs, entering facilities without undergoing proper screening processes, or using counterfeit TWICs. We note that these issues are taken seriously, but are outside the scope of this rulemaking as we are not changing the actions to be taken upon identification of TWIC issues, merely how they might be detected.

One commenter noted that ''terminals must abide by common law and practice,'' in reference to the idea that TWICs are not the sole condition of entry. The Coast Guard agrees, but notes the improvement in access control that electronic TWIC inspection provides.

One commenter implied that ammonium nitrate should not be considered CDC. Altering the list of CDC (defined in 33 CFR part 160) is beyond the scope of this rulemaking.

One commenter noted that visual TWIC inspection presents a safety issue, as security personnel can be injured or killed by vehicles approaching the gate area. While there are certainly security incidents where attackers can try to use force to breach the perimeter of a secure facility, such incidents are beyond the scope of this rule.

One commenter suggested that the U.S. Congress should fully fund the TWIC reader program, and asserted that funding of Federally mandated programs will ensure a degree of financial relief and minimize burdens. While we agree that funding would shift the industry burden to taxpayers, this comment remains beyond the scope of this rule.

Finally, this final rule makes a number of minor, technical edits, including updating internal references, to the regulations in 33 CFR Chapter I, Subchapter H, in addition to the changes discussed elsewhere in the preamble. These edits affect the following sections in Title 33 of the CFR:

- 101.105 Definitions.
- 101.514 TWIC Requirement.
- 101.515 TWIC/Personal Identification.
- 104.105 Applicability.
- 104.115 Compliance.
- 104.120 Compliance documentation.
- 104.200 Owner or operator.
- 104.215 Vessel Security Officer (VSO).
- 104.235 Vessel recordkeeping requirements.
- 104.260 Security systems and equipment maintenance.
- 104.267 Security measures for newly hired employees.
- 104.292 Additional requirements—passenger vessels and ferries.
- 104.405 Format of the Vessel Security Plan (VSP).
- 104.410 Submission and approval.
- 105.115 Compliance dates.
- 105.120 Compliance documentation.
- 105.200 Owner or operator.
- 105.257 Security measures for newly hired employees.
- 105.290 Additional requirements—cruise ship terminals.
- 105.296 Additional requirements—barge fleeting facilities.
- 105.405 Format and content of the Facility Security Plan (FSP).
- 105.410 Submission and approval.
- 106.110 Compliance dates.
- 106.115 Compliance documentation.
- 106.200 Owner or operator.
- 106.262 Security measures for newly-hired employees.
- 106.405 Format and content of the Facility Security Plan (FSP).
- 106.410 Submission and approval.

## VI. Regulatory Analyses

We developed this rule after considering numerous statutes and Executive Orders (E.O.s) related to rulemaking. Below we summarize our analyses based on these statutes or E.O.s.

### *A. Regulatory Planning and Review*

E.O.s 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). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This final rule is a significant regulatory action under section 3(f) of E.O. 12866. The Office of Management and Budget (OMB) has reviewed it under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of E.O. 12866. A final assessment is available in the docket, and a summary follows.

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

Table 3 summarizes the costs and benefits of this final rule.

TABLE 3—SUMMARY OF COSTS AND BENEFITS [64]

| Category | Final rule |
|---|---|
| Applicability | High-risk MTSA-regulated facilities and high risk MTSA-regulated vessels with greater than 20 TWIC-holding crew. |
| Affected Population | 1 vessel.<br>525 facilities. |
| Costs ($ millions, 7% discount rate) | $21.9 (annualized).<br>$153.8 (10-year). |
| Costs (Qualitative) | Time to retrieve or replace lost PINs for use with TWICs. |
| Benefits (Qualitative) | Enhanced access control and security at U.S. maritime facilities and on board U.S.-flagged vessels.<br>Reduction of human error when checking identification and manning access points. |

Table 4 summarizes the changes in the regulatory analysis as we moved from the NPRM to this final rule. These changes to the RA came from either policy changes on the electronic TWIC inspection requirements, public comments received after the publication of the NPRM in March 2013, or simply from updating the data and information that informed our regulatory analysis.

TABLE 4—CHANGES IN REGULATORY ANALYSIS FROM NPRM TO FINAL RULE

| Element of regulatory analysis | Reason changed | Explanation of change |
|---|---|---|
| Affected Population | Policy change | a. Barge fleeting facilities were removed reducing the previous facility population of 532 to 525, and<br>b. Crew size changed to 20 (instead of 14) and thus reducing the number of vessels to 1. |
| Cost of TWIC Readers | Update to reflect current prices for TWIC readers. | The most recent prices of electronic TWIC readers as published in GSA schedule and TSA's QTL were significantly reduced. |
| | Comments received | Some public comments suggested that TWIC reader costs have declined since the NPRM RA data was collected. |
| Wages for transportation workers | More current BLS data | Revised labor cost by using May 2012 BLS data. |
| Maintenance Cost of TWIC Readers. | Comment received | Revised this cost assumption from 5% of the total cost of a TWIC Reader to 10%. |
| Number of TWIC Readers | Comment received | Per one large ferry passenger facility's suggestion, accommodated this facility's higher number of readers in cost estimates. |

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

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

We estimate that this final rule would specifically affect owners and operators of certain 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, including barge fleeting facilities, that handle or receive vessels carrying CDC in bulk; and (2) Facilities that receive vessels certificated to carry more than 1,000 passengers. 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 an electronic TWIC inspection exemption for vessels with 20 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 final rule and data from the Coast Guard's MISLE database, we estimate this final rule will affect 525 facilities and 1 vessel with additional costs. All of these facilities and vessels are in Risk Group A.

The final rule adds flexibility in using existing PACS to comply with the electronic TWIC inspection requirements, which may result in lower costs for affected facilities and vessels. For the purposes of regulatory analysis, however, we prepare the cost estimate assuming that all of the affected population will install and use electronic TWIC readers. The following discussion of the cost analysis is based on this assumption.

To estimate the costs for this proposal, we use data from a variety of sources, including MISLE, TWIC Pilot Study, TSA's ICE and QTL lists, public comments, and the GSA schedule among others. When data from the TWIC pilot are used (to estimate the costs for installation, integration, and PACS integration), the data are broken down by per electronic reader cost for each facility type. 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 applying the costs to the full affected population of this rulemaking.

The primary cost driver for this final 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, updates of the list of cancelled TWICs, 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 5 summarizes our estimates for total capital costs by facility type during the 2-year implementation period; Table 6 provides the operational costs for facilities by four requirements throughout the analysis period.[65]

[64] For a more detailed discussion of costs and benefits, see the full RA available in the online 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.

[65] See RA Tables 4.10 and 4.16 and associated discussion for the specific sources for our estimates as well as how they were developed.

TABLE 5—TOTAL FACILITY CAPITAL COSTS, 2-YEAR IMPLEMENTATION PERIOD (YEAR 1 AND YEAR 2)

| Facility type | Number | Total readers | | Total reader costs ($) | | Total costs ($) | | | Total capital cost ($) |
|---|---|---|---|---|---|---|---|---|---|
| | | Fixed | Portable | Fixed | Portable | Install. | Infra-structure | PACS | |
| Bulk Liquid ... | 290 | 1,535 | 292 | 8,247,555 | 2,054,220 | 11,475,387 | 20,033,055 | 15,279,201 | 57,089,418 |
| Break Bulk and Solids | 16 | 91 | 45 | 488,943 | 316,575 | 904,128 | 3,724,904 | 2,938,552 | 8,373,102 |
| Container ..... | 3 | 36 | 8 | 193,428 | 56,280 | 909,612 | 589,952 | 1,020,184 | 2,769,456 |
| Large Passenger ..... | 92 | 42 | 524 | 225,666 | 3,686,340 | 1,682,152 | 4,102,368 | 841,642 | 10,538,168 |
| Small Passenger ..... | 63 | 0 | 426 | 0 | 2,996,910 | 0 | 0 | 0 | 2,996,910 |
| Mixed Use .... | 61 | 180 | 72 | 967,140 | 506,520 | 8,191,008 | 6,300,000 | 1,242,108 | 17,206,776 |
| Total ..... | 525 | 1,884 | 1,367 | 10,122,732 | 9,616,845 | 23,162,287 | 34,750,279 | 21,321,687 | 98,973,830 |

TABLE 6—ANNUAL OPERATIONAL COSTS FOR FACILITIES

| Years after publication | Amend-ments | Recordkeeping | Canceled card list | Training | | Total |
|---|---|---|---|---|---|---|
| | | | | Personnel | FSO | |
| 1 | $467,614 | $748,182 | $486,319 | $209,219 | $74,676 | $1,986,009 |
| 2 | 465,836 | 857,138 | 484,469 | 261,523 | 93,345 | 2,162,312 |
| 3 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 4 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 5 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 6 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 7 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 8 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 9 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| 10 | 0 | 224,028 | 970,788 | 104,609 | 37,338 | 1,336,763 |
| Total | 933,450 | 3,397,544 | 8,737,092 | 1,307,616 | 466,725 | 14,842,427 |

Table 7 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. These costs are reduced from those estimated in the NPRM given cost reductions in TWIC readers and the removal of TWIC reader requirements for barge fleeting areas.

TABLE 7—10-YEAR TOTAL COSTS, BY FACILITY TYPE*

[$ Millions]

| Year | Bulk liquid | Break bulk and solids | Container | Large passenger | Small passenger | Mixed use | Total |
|---|---|---|---|---|---|---|---|
| 1 | $31.6 | $2.4 | $0.8 | $9.8 | $7.4 | $4.4 | $56.3 |
| 2 | 32.3 | 2.4 | 0.8 | 10.0 | 7.5 | 4.5 | 57.4 |
| 3 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| 4 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| 5 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| 6 | 10.1 | 0.8 | 0.2 | 3.1 | 2.4 | 1.4 | 18.0 |
| 7 | 10.1 | 0.8 | 0.2 | 3.1 | 2.4 | 1.4 | 18.0 |
| 8 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| 9 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| 10 | 4.6 | 0.3 | 0.1 | 1.4 | 1.1 | 0.6 | 8.1 |
| Total Undiscounted | 111.5 | 8.3 | 2.7 | 34.5 | 26.0 | 15.4 | 198.3 |
| Total Discounted at 7% | 88.7 | 6.6 | 2.1 | 27.5 | 20.7 | 12.2 | 157.8 |
| Total Discounted at 3% | 100.4 | 7.5 | 2.4 | 31.1 | 23.4 | 13.9 | 178.7 |

**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 final RA 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 electronic TWIC inspection requirements, we estimate a cost associated with failed reads.[66] 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 electronic TWIC inspection transaction would lead to the use of a secondary processing operation, such as a visual TWIC inspection, additional identification validation, or other provisions as set forth in the FSP.[67]

Table 8 provides the annual costs associated with delays caused by invalid transactions for Risk Group A Facilities.

TABLE 8—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 | $94,339 | $188,678 | $283,017 | $377,356 | $471,696 | $283,017 |
| 14 Seconds | 220,125 | 440,249 | 660,374 | 880,498 | 1,100,623 | 660,374 |
| 30 Seconds | 471,696 | 943,391 | 1,415,087 | 1,886,782 | 2,358,478 | 1,415,087 |
| 60 Seconds | 943,391 | 1,886,782 | 2,830,173 | 3,773,564 | 4,716,955 | 2,830,173 |
| 120 Seconds | 1,886,782 | 3,773,564 | 5,660,346 | 7,547,129 | 9,433,911 | 5,660,346 |
| Average | 723,266 | 1,446,533 | 2,169,799 | 2,893,066 | 3,616,332 | 2,169,799 |

For the purposes of this analysis, we used the cost of delay estimate of $2.2 million per year, which represents the average delay across all iterations of delay times and electronic TWIC inspection transactions.

The use of TWIC readers will 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.[68] 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 may result 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 each year 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 $254.93 per TWIC-holder to travel to a TWIC Enrollment center and get a replacement TWIC.[69] Overall, we estimate that TWIC replacement would cost approximately $2.3 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 9 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 9—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 | $107,907 | $145,588 | $251,211 | $105,375 | $115,818 | $ 70,758 |
| Annual Recurring Cost | 14,575 | 19,664 | 33,931 | 14,233 | 15,643 | 9,557 |
| Annual Recurring Cost *with* Equipment Replacement | 33,701 | 45,470 | 78,457 | 32,910 | 36,172 | 22,099 |

For the single Risk Group A vessel with greater than 20 TWIC-holding crewmembers, we assume that this vessel will comply with the requirements by purchasing two portable TWIC readers (total first year cost of $14,070) and deploying them at the main access points of the vessel, replacing them at Year 6. We also estimate $1,339 for VSP amendments; $2,142 for the development of a recordkeeping system; and $2,028 for training in Year 1. Recurring costs include updates of the list of cancelled TWICs ($1,392 per year), ongoing training ($507 per year), and ongoing recordkeeping ($321 per year). We estimate the annualized costs to vessels of this rulemaking to be approximately $7,270 at a 7 percent discount rate. These costs are shown in Table 10.

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

[67] The final RA 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.

[68] 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.

[69] This cost is explained in greater detail in the Final Regulatory Analysis and Final Regulatory Flexibility Analysis. It includes an estimated $194.93 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 chose to travel to a TWIC Enrollment Center to get a replacement TWIC instead of waiting to receive it by mail.

TABLE 10—TOTAL VESSEL COSTS (RISK GROUP A WITH MORE THAN 20 TWIC-HOLDING CREWMEMBERS) *

| Year | Undiscounted | 7% | 3% |
|---|---|---|---|
| 1 | $20,971 | $19,599 | $20,360 |
| 2 | 3,627 | 3,168 | 3,419 |
| 3 | 3,627 | 2,961 | 3,319 |
| 4 | 3,627 | 2,767 | 3,222 |
| 5 | 3,627 | 2,586 | 3,129 |
| 6 | 17,697 | 11,792 | 14,821 |
| 7 | 3,627 | 2,259 | 2,949 |
| 8 | 3,627 | 2,111 | 2,863 |
| 9 | 3,627 | 1,973 | 2,780 |
| 10 | 3,627 | 1,844 | 2,699 |
| Total | 67,682 | 51,058 | 59,560 |
| Annualized | | 7,270 | $,982 |

* Because the affected population is only one vessel, we assume that this vessel will comply within the first year of implementation.

We estimate the annualized cost of this final rule to industry over 10 years to be approximately $21.9 million at a 7 percent discount rate. The main cost drivers of this final rule are the acquisition and installation of TWIC readers and the maintenance of the affected entity's electronic TWIC inspection system. Initial costs, which will 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 will be driven by costs associated with updates of the list of cancelled TWICs, recordkeeping, training, system maintenance and opportunity costs associated with failed TWIC reader transactions.

We estimated the present value average costs of this final rule on industry for a 10-year period as summarized in Table 11. The costs were discounted at 3 and 7 percent as set forth by guidance in OMB Circular A–4.

TABLE 11—TOTAL INDUSTRY COST, RISK GROUP A

[$ Millions]

| Year | Facility | Vessel | Additional costs * | Undiscounted | 7% | 3% |
|---|---|---|---|---|---|---|
| 1 | $51.5 | $0.0 | $4.8 | $56.3 | $52.6 | $54.7 |
| 2 | 52.6 | 0.0 | 4.8 | 57.4 | 50.2 | 54.1 |
| 3 | 3.3 | 0.0 | 4.8 | 8.1 | 6.6 | 7.4 |
| 4 | 3.3 | 0.0 | 4.8 | 8.1 | 6.2 | 7.2 |
| 5 | 3.3 | 0.0 | 4.8 | 8.1 | 5.8 | 7.0 |
| 6 | 13.2 | 0.0 | 4.8 | 18.0 | 12.0 | 15.1 |
| 7 | 13.2 | 0.0 | 4.8 | 18.0 | 11.2 | 14.6 |
| 8 | 3.3 | 0.0 | 4.8 | 8.1 | 4.7 | 6.4 |
| 9 | 3.3 | 0.0 | 4.8 | 8.1 | 4.4 | 6.2 |
| 10 | 3.3 | 0.0 | 4.8 | 8.1 | 4.1 | 6.0 |
| Total | 150.3 | 0.1 | 48.0 | 198.4 | 157.8 | 178.8 |
| Annualized | | | | | 22.5 | 21.0 |

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

As this final rule will require amendments to FSPs and VSPs, we estimate a cost to the government to review these amendments during the implementation period, but do not anticipate any further annual cost to the government from this final rule. For the total implementation period, the total government cost will be $93,177 at a 7 percent discount rate. Table 12 shows the 10-year government costs.

TABLE 12—GOVERNMENT COSTS *

| Year | FSP | VSP | Total undiscounted | 7% | 3% |
|---|---|---|---|---|---|
| 1 | $51,450 | $166 | $51,616 | $48,239 | $50,112 |
| 2 | 51,450 | 0 | 51,450 | 44,938 | 48,497 |
| 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 |

TABLE 12—GOVERNMENT COSTS *—Continued

| Year | FSP | VSP | Total undiscounted | 7% | 3% |
|---|---|---|---|---|---|
| Total | 102,900 | 166 | 103,066 | 93,177 | 98,609 |
| Annualized | | | 13,266 | | 11,560 |

* 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 provisions in this final rule and recent data, we estimated the average first-year cost of this final rule (combined industry and government) to be approximately $52.1 million or $54.1 million at a 7 or 3 percent discount rate, respectively. The undiscounted annual recurring cost for this final rule is approximately $7.5 million in every year except years 6 and 7, due to equipment replacement 5 years after implementation. The annualized cost of this final rule is $21.9 million at 7 percent and $20.4 million at 3 percent. The 10-year cost to industry and government of this final rule is approximately $153.8 million at a 7 percent discount rate, and $173.9 million at a 3 percent discount rate.

The benefits of the final 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 and reducing regulatory uncertainty by closing the gap between MTSA and SAFE Port Act requirements for electronic TWIC inspection and regulatory requirements.

Electronic TWIC inspection programs 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.

Data limitations preclude us monetizing these benefits, but instead, we use break-even analysis. Break-even analysis is useful when it is not possible to quantify the benefits of a regulatory action. OMB Circular A–4 recommends a ''threshold'' or ''break-even'' analysis when non-quantified benefits are important to evaluating the benefits of a regulation. 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?'' [70] 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 electronic TWIC inspection 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 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 electronic TWIC inspection programs. These scenarios were chosen because they represent the scenarios most likely to benefit from the enhanced access control afforded by electronic TWIC inspection, 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 electronic TWIC inspection 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.

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 regulatory 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 premature death. We currently use a value of $9.1 million as an estimate of VSL.[71] 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.

[70] U.S. Office of Management and Budget, Circular A–4, September 17, 2003, page 2.

[71] See the Department of Transportation's ''*Guidance on the Treatment of the Economic Value of a Statistical Life in U.S. Department of Transportation Analyses*'' *http://www.dot.gov/sites/dot.dev/files/docs/VSL%20Guidance%202013.pdf.*

TABLE 13—ANNUAL RISK REDUCTION AND ATTACKS AVERTED REQUIRED FOR COSTS TO EQUAL BENEFITS, FINAL RULE ALTERNATIVE

| | Annualized cost, 7% discount rate ($ Millions) | Average maximum consequence ($ Millions) | Required reduction in risk to break-even | Frequency of attacks averted to break-even |
|---|---|---|---|---|
| Final Rule Alternative | $21.9 | $5,014.1 | 0.4% | One every 229 years |

As shown in Table 13, an avoided terrorist attack at an average target is equivalent to $5.01 billion in avoided consequences. This final rule is estimated to cost approximately $21.9 million annually. 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 0.5 percent. To state this in another way, if implementing this regulation will lower the likelihood of a successful terrorist attack by more than 0.4 percent each year, then this would be a socially efficient use of resources. This final rule would be cost effective if it prevented one terrorist attack with consequence equal to the average every 229 years ($5,014.1/$21.9). These small changes in required risk reduction suggest that the potential benefits of the final rule justify the costs.

For the final rule alternative, we assess that all Risk Group A facilities will be required to conduct electronic TWIC inspections. On the vessel side, we assess that all Risk Group A vessels with a crew size greater than 20 TWIC-holding crewmembers will likely carry two portable TWIC readers. For this alternatives analysis, we look at several different ways to implement electronic TWIC inspection 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 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 14 summarizes the cost of the alternatives considered. The costs displayed are the 10-year costs and the 10-year annualized cost, each discounted at 7 percent.

TABLE 14—REGULATORY ALTERNATIVES

| | Description | Facility population | Vessel population | Total cost ($ millions, at 7% discount rate) | Annualized cost ($ millions, at 7% discount rate) |
|---|---|---|---|---|---|
| Final Rule Alternative | All Risk Group A facilities and Risk Group A vessels with more than 20 crewmembers. | 525 | 1 | $153.8 | $21.9 |
| NPRM Alternative | All Risk Group A facilities and Risk Group A vessels with more than 14 crewmembers. | 532 | 38 | 153.5 | 21.9 |
| Alternative 2 | All Risk Group A facilities and Risk Group A vessels (except barges). | 532 | 138 | 158.2 | 22.5 |
| Alternative 3 | Risk Group A and all container facilities and Risk Group A vessels with more than 14 crewmembers. | 651 | 38 | 182.6 | 26.0 |
| 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 | 309.5 | 44.1 |
| Alternative 5 (ANPRM Alternative) | Risk Group A and B Facilities and Risk Group A vessels with more than 14 crewmembers. | 2,173 | 38 | 548.9 | 78.1 |

When comparing alternatives, we also looked at the results of the break-even analysis for these alternatives. As Table 15 shows, for the overall average maximum consequence, the final rule alternative will 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 15—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 | Frequency of attacks averted |
|---|---|---|---|---|
| Final Rule Alternative | $21.9 | $5,014.10 | 0.44% | One every 229 years. |
| NPRM Alternative | 21.9 | 5,014.10 | 0.44% | One every 229.0 years. |
| Risk Group A facilities and all Risk Group A vessels, except barges | 22.5 | 5,014.10 | 0.45% | One every 222.8 years. |
| Risk Group A and all container facilities and Risk Group A vessels with more than 14 crewmembers. | 26.0 | 4,158.7 | 0.63% | One every 160.0 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. | 44.1 | 2,211.3 | 1.99% | One every 50.1 years. |
| ANPRM Alternative Risk Groups A and B facilities and Risk Group A vessels with more than 14 crewmembers. | 78.1 | 1,647.1 | 4.74% | One every 21.1 years. |

Final rule Alternative—Risk Group A Facilities and Risk Group A Vessels with More than 20 TWIC-Holding Crewmembers:

The analysis for this alternative is discussed in detail previously in this section, as it is the alternative we have chosen in this final rule.

NPRM Alternative—Risk Group A Facilities and Risk Group A Vessels with More than 14 TWIC-Holding Crewmembers:

The analysis for this alternative was discussed in detail in the previously published NPRM's regulatory impact analysis.[72] The two key differences between the final rule and NPRM alternative are the exemption of barge fleeting facilities reducing the affected facility population to 525 and the adoption of the crew size of 20 or more removing all vessels except one in the final rule as opposed to all 532 facilities and 38 vessels in the Risk Group A.

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

This alternative would require electronic TWIC inspection 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 1 vessel 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 remain the same at $21.9 million, at a 7 percent discount rate. The discounted 10-year costs would go from $157.9 million to $158.2 million. While this alternative does not lead to a significant increase in costs, we reject it because requiring electronic TWIC inspection 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 in the NPRM, and was based on a recommendation from TSAC. See the discussion in the NPRM on ''Recurring Unescorted Access'' and ''TWIC Reader Exemption for Vessels with 14 or Fewer TWIC-Holding Crewmembers'' for more details.[73]

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 electronic TWIC inspection. This alternative would increase the burden on industry and small entities by increasing the affected population from 525 facilities to 651 facilities. Under this scenario, the annualized cost of this rulemaking would increase from $21.9 million to $26.0 million, at a 7 percent discount rate. The discounted 10-year costs would go from $153.8 million to $182.6 million. The inclusion of container facilities would also potentially have adverse environmental impacts due to increased air emissions due to longer wait (''queuing'') times and congestion at facilities.

We considered this alternative because of the risk associated with container facilities due to the transfer risk associated with containers. As discussed in the preamble of the NPRM, many of the high-risk threat scenarios at container facilities would not be mitigated by electronic TWIC inspection. The costs for electronic TWIC inspection at container facilities would not be justified by the amount of potential risk reduction at these facilities from such a measure. While container facilities pose a higher 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 electronic TWIC inspection serves as an additional access control measure, but would not improve screening of cargoes for dangerous substances or devices.

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 525 facilities to 1,174 facilities. Under this scenario, the annualized cost of this rulemaking would increase from $21.9 million to $44.1 million, at a 7 percent discount rate. The discounted 10-year costs would go from $153.8 million to $309.5 million.

We considered this alternative based on the high MSRAM consequences

[72] 78 FR 17782.

[73] 78 FR 17803 and 78 FR 17813, respectively.

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 consequences for these facility types, the overall risk as determined in the 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 electronic TWIC inspection 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 525 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 $21.9 million to $78.1 million, at a 7 percent discount rate. The discounted 10-year costs would go from $153.8 million to $548.9 million. Based on a recent study by the Homeland Security Institute, as discussed in the preamble to the 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 final rule alternative. For these reasons, we rejected this alternative.

The provisions in this final rule are taken in order to meet requirements set forth in MTSA and the SAFE Port Act. The final rule, 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.

Furthermore, by allowing for flexibilities, such as the use of fixed or portable TWIC readers, and removing vessels with 20 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 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 less than 50,000. A Final Regulatory Flexibility Analysis discussing the impact of this final rule on small entities is available in the docket, and a summary follows.

For this final rule, we estimated costs for mandatory electronic TWIC inspection for approximately 1 vessel and 525 facilities based on the risk assessment hierarchy and current data from the Coast Guard's MISLE database. Of these 525 facilities that would be affected by the electronic TWIC inspection requirements, we found 306 unique owners. Among these 306 unique owners, there were 31 government-owned entities, 114 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 final rule, 24 exceed the 50,000 population threshold as defined by the Regulatory Flexibility Act to be considered small, and the remaining 7 have government revenue levels such that there would not be an impact greater than 1 percent of government revenue.[74]

We were able to find revenue information for 64 of the 88 businesses deemed small by SBA size standards.[75] We then determined the impacts of the final rule on these companies by comparing the cost of the final 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 final rule will have based on implementation costs (including capital costs) and annual recurring costs (including updates of the list of cancelled TWICs, recordkeeping, and training). We estimate these costs to be, on average $195,715 per entity during the implementation period and $12,612 per entity in annual recurring cost.[76] The actual cost faced by a specific facility will vary based on a number of factors, such as the number of access points. Smaller facilities should in general incur lower costs, but the Coast Guard is unable to distinguish cost estimates on a facility-by-facility basis. We note that in some cases owners and operators might be able to finance the equipment costs as needed and such financing scenario could further decrease the impact on the facility owner and operators. We base our impact analysis on average cost to regulated entities due to the flexibility afforded by this final rule to individual facilities to determine how best to implement electronic TWIC inspection requirements.[77] Table 16 shows the potential revenue impacts for small businesses impacted by this final rule.

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

[75] 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.

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

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

TABLE 16—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% | 33 | 52 | 57 | 89 |
| 1% < Impact ≤ 3% | 4 | 6 | 6 | 9 |
| 3% < Impact ≤ 5% | 5 | 8 | 0 | 0 |
| 5% < Impact ≤ 10% | 8 | 13 | 1 | 2 |
| Above 10% | 14 | 22 | 0 | 0 |
| Total | 64 | 100 | 64 | 100 |

The greatest impact is expected to occur during the implementation phase when 48 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 3 percent of businesses would see an impact greater than 1 percent, and 0 percent would see an impact greater than 10 percent.[78]

For vessels, we found that for the 1 vessel that will be affected by this final rule, there is 1 unique owner that did not qualify as small business by SBA size standards. Therefore, we do not provide a revenue impact analysis for affected small business as we provided above for affected facilities.

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996, Public Law 104–121, we offered to assist small entities in understanding this rule so that they could better evaluate its effects on them and participate in the rulemaking. The Coast Guard will not retaliate against small entities that question or complain about this rule or any policy or action of the Coast Guard.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1–888–REG–FAIR (1–888–734–3247).

*D. Collection of Information*

This rule calls for a collection of information under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501–3520. You are not required to respond to a collection of information unless it displays a currently valid OMB control number. As required by 44 U.S.C. 3507(d), we submitted a copy of the final rule to the OMB for its review of the collection of information. 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 completing and reviewing the collection.

Under the provisions of the final rule, the affected facilities and vessel will 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 will 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 final rule will require certain vessel and facilities to use electronic readers designed to work with the TWIC as an access control measure. Affected owners and operators will also face requirements associated with electronic TWIC inspection, 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 electronic TWIC inspection requirements.

*Proposed Use of Information:* We will use this information to ensure that facilities and vessels are properly implementing and utilizing electronic TWIC inspection programs.

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

*Number of Respondents:* The number of respondents is the 525 facilities that are considered ''high-risk'' and would be required to modify their existing FSPs, and 1 vessel that would be required to modify its VSP to account for the electronic TWIC inspection requirements. These same populations will 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 will need to be met along a similar timeline.

*Burden of Response:* The estimated burden for facilities would be 17,063 hours in the first year, 17,063 hours in the second year and 3,150 hours in the third year and all subsequent years. The burden for vessels would be 65 burden

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

hours in year one, and 6 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 list of cancelled TWICs.

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 525 facilities that will need to amend their FSPs, the total burden on facilities would be 13,125 hours (525 FSPs × 25 hours per amendment) during the 2-year implementation period, or 6,563 hours each of the first 2 years. Facilities would also face a recordkeeping burden of 21,000 hours during the 2-year implementation period (525 facilities × 40 hours per recordkeeping system), or 10,500 hours each year over the first 2 years. There would also be an annual recordkeeping burden of 3,150 hours (525 facilities × 6 hours per year), starting in the third year. In the second year, the 262 facilities that implemented in the first year would incur the 6 hours of annual recordkeeping, at a burden of 1,572 (262 facilities × 6 hours). The total burden for facilities is estimated at 17,063 (6,563 + 10,500) in Year 1, 17,063 in Year 2 (6,563 + 10,500), and 3,150 in Year 3.

*Vessels:* For the 1 vessel, the burden in the first year would be 25 hours (1 VSP × 25 hour per amendment). Vessels would also face a recordkeeping burden of 40 hours during the 1-year implementation period (1 vessel × 40 hours per recordkeeping system). There would also be an annual recordkeeping burden of 6 hours, starting in Year 2, (1 vessel × 6 hours per year). The total burden for vessels is estimated at 65 (25 + 40) in Year 1 and 6 hours in Years 2 and 3.

*Total:* The total additional burden due to the electronic TWIC inspection rule is estimated at 17,128 (65 for vessels and 17,063 for facilities) in Year 1, 17,069 (6 for vessel and 17,063 for facilities) in Year 2, and 3,156 (6 for vessels and 3,150 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 final rule, in Year 1 is 1,125,171 (1,108,043 + 17,128). In Year 2, the new burden, as a result of this final rule, is 1,125,171 (1,108,043 + 17,128) and in Year 3 it is 1,111,199 (1,108,043 + 3,156). The average annual additional burden across the 3 years is 12,425.

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

*E. Federalism*

A rule has implications for Federalism under E.O. 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 final rule has been analyzed in accordance with the principles and criteria in E.O. 13132, and it has been determined that this final rule does have Federalism implications or a substantial direct effect on the States.

This final 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 will be required to use TWIC readers. Additionally, this final rule will 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 final rule since it will require certain MTSA-regulated vessels to carry TWIC readers or a PACS that can conduct electronic TWIC inspection (*i.e.,* required equipment), and to conform to recordkeeping and security plan requirements. In enacting MTSA, Congress articulated a need to address nationwide port security threats while preserving the free flow of interstate and international maritime commerce. Congress identified enhancing global maritime security through implementing international security instruments as furthering this statutory purpose. MTSA's comprehensive and uniform maritime security regime, founded on the purpose of facilitating interstate and international maritime commerce, indicates that States and local governments are generally foreclosed from regulating within this field. As discussed above, vessel equipping and operation are traditionally fields foreclosed from State and local regulation. However, States and local governments have traditionally shared certain regulatory jurisdiction over waterfront facilities. Therefore, MTSA standards contained in 33 CFR part 105 (Maritime security: Facilities) are not preemptive of State or local law or regulations that do not conflict with them (*i.e.,* they would either actually conflict or would frustrate an overriding Federal need for uniformity).

The Coast Guard recognizes the key role that State and local governments may have in making regulatory determinations. Additionally, Sections 4 and 6 of E.O. 13132 require that for any rules with preemptive effect, the Coast Guard 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 consult with such officials early in the rulemaking process. Therefore, we invited 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 the NPRM.

Numerous State and local governments responded to the Coast Guard's invitation by actively participating in this rulemaking process. State and local government interests participated by submitting written comments and by attending and presenting their views in person at four public meetings we held across the country to solicit comments on this rulemaking. All comments have been posted to the docket for this rulemaking. Participating State and local government interests included: Alaska Marine Highway System; American Association of Port Authorities; Broward County, Florida Port Everglades Department; Calhoun Port Authority; King County, Washington Department of Transportation; New York City Department of Transportation; Port Authority of New York and New Jersey; Port of Galveston; Port of Houston Authority; Port of Seattle; Port of Stockton; Port of Tacoma; and

Washington State Department of Transportation. We considered this State and local government input in the promulgation of this final rule, and multiple changes to the final rule are attributable to these comments. Based on these consultations and the content of the final rule, we can ensure that the final rule is consistent with the fundamental federalism principles and preemption requirements described in E.O. 13132.

*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 rule will not result in such an expenditure, we do discuss the effects of this rule elsewhere in this preamble.

*G. Taking of Private Property*

This rule will not cause a taking of private property or otherwise have taking implications under E.O. 12630 (''Governmental Actions and Interference with Constitutionally Protected Property Rights'').

*H. Civil Justice Reform*

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

*I. Protection of Children*

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

*J. Indian Tribal Governments*

This rule does not have tribal implications under E.O. 13175 (''Consultation and Coordination with Indian Tribal Governments''), because it would not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

*K. Energy Effects*

We have analyzed this rule under E.O. 13211 (''Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use''). We have determined that it is not a ''significant energy action'' under E.O. 13211, because although it is a ''significant regulatory action'' under E.O. 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy, and the Administrator of OMB's Office of Information and Regulatory Affairs has not designated it as a significant energy action.

*L. Technical Standards*

The National Technology Transfer and Advancement Act (NTTAA), codified as a note to 15 U.S.C. 272, directs agencies to use voluntary consensus standards in their regulatory activities unless the agency provides Congress, through OMB, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (*e.g.,* specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies.

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

The Federal government is constantly working on improving electronic TWIC inspection 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 and TSA have established the QTL and the associated standards for identity and privilege credential products, to be managed by TSA. NIST continues to assist TSA with the development of testing suites for qualifying products in conformity to specified standards and TSA specifications.

*M. Environment*

We have analyzed this rule under Department of Homeland Security Management Directive 023–01 and Commandant Instruction M16475.lD, which guide the Coast Guard in complying with the National Environmental Policy Act of 1969, 42 U.S.C. 4321–4370f, and have concluded that this action is not likely to have a significant effect on the human environment. A Final Programmatic Environmental Assessment and a final Finding of No Significant Impact are available in the docket for this rulemaking. Our analysis indicates that electronic TWIC inspection operations will have insignificant direct, indirect or cumulative impacts on environmental resources, with special attention to potential air quality issues.

**List of Subjects**

*33 CFR Parts 101 and 103*

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, the Coast Guard amends 33 CFR parts 101, 103, 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 the definitions, in alphabetical order, of ''biometric match''; ''Canceled Card List (CCL)''; ''Card Holder Unique Identifier (CHUID)''; ''card validity check''; ''Designated Recurring Access Area (DRAA)''; ''electronic TWIC inspection''; ''identity verification''; ''Mobile Offshore Drilling Unit (MODU)''; ''Non-TWIC visual identity verification;'' ''Offshore Supply Vessel (OSV)''; ''Physical Access Control System (PACS)''; ''Qualified Reader''; ''Risk Group''; ''Transparent Reader''; ''TWIC reader''; and ''visual TWIC inspection''; and

■ b. Revise the definitions of ''bulk or in bulk''; ''recurring unescorted access''; and ''TWIC Program''.

The revisions and additions read as follows:

**§ 101.105 Definitions.**

* * * * *

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

* * * * *

*Bulk* or *in bulk* means a commodity that is loaded or carried without containers or labels, and that is received and handled without mark or count. This includes cargo transferred using hoses, conveyors, or vacuum systems.

* * * * *

*Canceled Card List (CCL)* is a list of 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 the card has been reported lost, stolen, or damaged.

* * * * *

*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 TSA-supplied list of cancelled TWICs or, for vessels and facilities not in Risk Group A, by verifying that the expiration date on the face of the TWIC has not passed.

* * * * *

*Designated Recurring Access Area (DRAA)* means an area designated under § 101.555 where persons are permitted recurring access to a secure area of a vessel or facility.

* * * * *

*Electronic TWIC inspection* means the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the stored biometric template.

* * * * *

*Identity verification* means the process by which an individual presenting a TWIC is verified as the owner of the TWIC.

* * * * *

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

* * * * *

*Non-TWIC visual identity verification* means the process by which an individual who is known to have been granted unescorted access to a secure area on a vessel or facility is matched to the picture on the facility's PACS card or a government-issued identification card.

* * * * *

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

* * * * *

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

* * * * *

*Qualified Reader* means an electronic device listed on TSA's Qualified Technology List that is capable of reading a TWIC.

*Recurring unescorted access* refers to special access procedures within a DRAA where a person may enter a secure area without passing an electronic TWIC inspection prior to each entry into the secure area.

* * * * *

*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 TWIC requirements in this subchapter.

* * * * *

*Transparent Reader* means a device capable of reading the information from a TWIC or individual seeking access and transmitting it to a system capable of conducting electronic TWIC inspection.

* * * * *

*TWIC Program* means those procedures and systems that a vessel, facility, or outer continental shelf (OCS) facility must implement in order to assess and validate TWICs when maintaining access control.

*TWIC reader* means a device capable of conducting an electronic TWIC inspection.

* * * * *

*Visual TWIC inspection* means the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the photograph on the face of the TWIC.

* * * * *

■ 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 by frustrating an overriding Federal need for uniformity.

**§ 101.514 [Amended]**

■ 4. Amend § 101.514 as follows:

■ a. In paragraph (b), remove the word ''federal'' and add, in its place, the word ''Federal''; and

■ b. In paragraph (d), remove the word ''State,'' and add, in its place, the word ''State''.

■ 5. Amend § 101.515 as follows:

■ a. In paragraph (a), remove the words ''of this part shall be required to'' and add, in their place, the words ''must'';

■ b. In paragraph (b)(1), remove the words ''of behalf'' and add, in their place, the words ''on behalf'';

■ c. In paragraph (c), remove the words ''of this part''; and

■ d. Revise paragraph (d)(2).

The revision reads as follows:

**§ 101.515 TWIC/Personal Identification.**

* * * * *

(d)* * *

(2) Each person who has been issued or possesses a TWIC must pass an electronic TWIC inspection, and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a Personal Identification Number, 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 subpart E to read as follows:

**§ 101.520 Electronic TWIC inspection.**

To conduct electronic TWIC inspection, the owner or operator of a vessel or facility must ensure the following actions are performed.

(a) *Card authentication.* The TWIC must be authenticated by performing a challenge/response protocol using the Certificate for Card Authentication (CCA) and the associated card authentication private key stored in the TWIC.

(b) *Card validity check.* The TWIC must be checked to ensure the TWIC has not expired and against TSA's list of cancelled TWICs, and no match on the list may be found.

(c) *Identity verification.* (1) One of the biometric templates stored in the TWIC must be matched to the TWIC-holder's

live sample biometric or, by matching to the PACS enrolled reference biometrics linked to the FASC–N of the TWIC; or

(2) If an individual is unable to provide a valid live sample biometric, the TWIC-holder must enter a Personal Identification Number (PIN) and pass a visual TWIC inspection.

■ 7. Add § 101.525 to subpart E to read as follows:

**§ 101.525 TSA list of cancelled TWICs.**

(a) At Maritime Security (MARSEC) Level 1, the card validity check must be conducted using information from the TSA that is no more than 7 days old.

(b) At MARSEC Level 2, the card validity check must be conducted using information from the TSA that is no more than 1 day old.

(c) At MARSEC Level 3, the card validity check must be conducted using information from the TSA that is no more than 1 day old.

(d) The list of cancelled TWICs used to conduct the card validity check must be updated within 12 hours of any increase in MARSEC level, no matter when the information was last updated.

(e) Only the most recently obtained list of cancelled TWICs must be used to conduct card validity checks.

■ 8. Add § 101.530 to subpart E to read as follows:

**§ 101.530 PACS requirements for Risk Group A.**

This section lays out requirements for a Physical Access Control System (PACS) that may be used to meet electronic TWIC inspection requirements.

(a) A PACS may use a TWIC directly to perform electronic TWIC inspection;

(b) Each PACS card issued to an individual must be linked to that individual's TWIC, and the PACS must contain the following information from each linked TWIC:

(1) The name of the TWIC-holder holder as represented in the Printed Information container of the TWIC.

(2) The TWIC-signed CHUID (with digital signature and expiration date).

(3) The TWIC resident biometric template.

(4) The TWIC digital facial image.

(5) The PACS Personal Identification Number (PIN).

(c) When first linked, a one-time electronic TWIC inspection must be performed, and the TWIC must be verified as authentic, valid, and biometrically matched to the individual presenting the TWIC.

(d) Each time the PACS card is used to gain access to a secure area, the PACS must—

(1) Conduct identity verification by:

(i) Conducting a biometric scan, and match the result with the biometric template stored in the PACS that is linked to the TWIC, or

(ii) Having the individual enter a stored PACS PIN and conducting a Non-TWIC visual identity verification as defined in § 101.105.

(2) Conduct a card validity check; and

(3) Maintain records in accordance with §§ 104.235(g) or 105.225(g) of this subchapter, as appropriate.

■ 9. Add § 101.535 to subpart E to read as follows:

**§ 101.535 Electronic TWIC inspection 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) *Requirements for Risk Group A vessels.* Prior to each boarding of the vessel, all persons who require access to a secure area of the vessel must pass an electronic TWIC inspection before being granted unescorted access to the vessel.

(b) *Requirements for Risk Group A facilities.* Prior to each entry into a secure area of the facility, all persons must pass an electronic TWIC inspection before being granted unescorted access to secure areas of the facility.

(c) A Physical Access Control System that meets the requirements of § 101.530 may be used to meet the requirements of this section.

(d) The requirements of this section do not apply under certain situations described in §§ 101.550 or 101.555.

(e) Emergency access to secure areas, including access by law enforcement and emergency responders, does not require electronic TWIC inspection.

■ 10. Add § 101.540 to subpart E to read as follows:

**§ 101.540 Electronic TWIC inspection requirements for vessels, facilities, and OCS facilities not in Risk Group A.**

A vessel or facility not in Risk Group A may use the electronic TWIC inspection requirements of § 101.535 in lieu of visual TWIC inspection. If electronic TWIC inspection is used, the recordkeeping requirements of §§ 104.235(b)(9) and (c) of this subchapter, or 105.225(b)(9) and (c) of this subchapter, as appropriate, apply.

**§ 101.545 [Added and Reserved]**

■ 11. Add reserved § 101.545 to subpart E.

■ 12. Add § 101.550 to subpart E to read as follows:

**§ 101.550 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 Transportation Worker Identification Credential (TWIC) Program is implemented as follows:

(a) *Lost, damaged, stolen, or expired TWIC.* If an individual cannot present a TWIC because it has been lost, damaged, stolen, or expired, and the individual previously has been granted unescorted access to secure areas and is known to have had a TWIC, the individual may be granted unescorted access to secure areas for a period of no longer than 30 consecutive calendar days if—

(1) The individual provides proof that he or she has reported the TWIC as lost, damaged, or stolen to the Transportation Security Administration (TSA) as required in 49 CFR 1572.19(f), or the individual provides proof that he or she has applied for the renewal of an expired TWIC;

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

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

(b) *TWIC on the Canceled Card List.* In the event an individual reports his or her TWIC as lost, damaged, or stolen, and that TWIC is then placed on the Canceled Card List, the individual may be granted unescorted access by a Physical Access Control System (PACS) that meets the requirements of § 101.530 for a period of no longer than 30 days. The individual must be known to have had a TWIC, and known to have reported the TWIC as lost, damaged, or stolen to TSA.

(c) *Special requirements for Risk Group A vessels and facilities.* If a TWIC reader or a PACS cannot read an individual's biometric templates due to poor biometric quality or no biometrics enrolled, the owner or operator may grant the individual unescorted access to secure areas based on either of the following secondary authentication procedures:

(1) The owner or operator must conduct a visual TWIC inspection and require the individual to correctly submit his or her TWIC Personal Identification Number.

(2) [Reserved]

(d) If an individual cannot present a TWIC for any reason other than those

outlined in paragraphs (a) or (b) of this section, the vessel or facility operator may not grant the individual unescorted access to secure areas. The individual must be under escort at all times while in the secure area.

(e) With the exception of individuals granted access according to paragraphs (a) or (b) of this section, all individuals granted unescorted access to secure areas of a vessel, facility, or OCS facility must be able to produce their TWICs upon request from the TSA, the Coast Guard, another authorized Department of Homeland Security representative, 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 operator should coordinate the TWIC Program, when practical, with identification and TWIC access control measures of other entities that interface with the vessel, facility, or OCS facility.

■ 13. Add § 101.555 to subpart E to read as follows:

**§ 101.555 Recurring Unescorted Access for Risk Group A vessels and facilities.**

This section describes how designated TWIC-holders may access certain secure areas on Risk Group A vessels and facilities on a continual and repeated basis without undergoing repeated electronic TWIC inspections.

(a) An individual may enter a secure area on a vessel or facility without undergoing an electronic TWIC inspection under the following conditions:

(1) Access is through a Designated Recurring Access Area (DRAA), designated under an approved Vessel, Facility, or Joint Vessel-Facility Security Plan.

(2) The entire DRAA is continuously monitored by security personnel at the access points to secure areas used by personnel seeking Recurring Unescorted Access.

(3) The individual possesses a valid TWIC.

(4) The individual has passed an electronic TWIC inspection within each shift and in the presence of the on-scene security personnel.

(5) The individual passes an additional electronic TWIC inspection prior to being granted unescorted access to a secure area if he or she enters an unsecured area outside the DRAA and then returns.

(b) The following requirements apply to a DRAA:

(1) It must consist of an unsecured area where personnel will be moving into an adjacent secure area repeatedly.

(2) The entire DRAA must be visible to security personnel.

(3) During operation as a DRAA, there must be security personnel present at all times.

(c) An area may operate as a DRAA at certain times, and during other times, access to secure areas may be obtained through the procedures in § 101.535.

(d) Personnel may enter the secure areas adjacent to a DRAA at any time using the procedures in § 101.535.

## PART 103—MARITIME SECURITY: AREA MARITIME SECURITY

■ 14. The authority citation for part 103 continues to read as follows:

**Authority:** 33 U.S.C. 1226, 1231; 46 U.S.C. 70102, 70103, 70104, 70112; 50 U.S.C. 191; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

**§ 103.505 [Amended]**

■ 15. Amend § 103.505(f) by removing the words ''(*e.g.,* TWIC)''.

## PART 104—MARITIME SECURITY: VESSELS

■ 16. 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]**

■ 17. Amend § 104.105(d) by removing the words ''this part'' and adding, in their place, the words ''parts 101 and 104 of this subchapter''.

■ 18. Add § 104.110(c) to read as follows:

**§ 104.110 Exemptions.**

* * * * *

(c) Vessels with a minimum manning requirement of 20 or fewer TWIC-holding crewmembers are exempt from the requirements in 33 CFR 101.535(a)(1).

■ 19. Amend § 104.115 as follows:

■ a. Revise paragraph (c); and

■ b. Remove paragraph (d).

The revision reads as follows:

**§ 104.115 Compliance.**

* * * * *

(c) By August 23, 2018, owners and operators of vessels subject to this part must amend their Vessel Security Plans to indicate how they will implement the TWIC requirements in this subchapter. By August 23, 2018, owners and operators of vessels subject to this part must operate in accordance with the TWIC provisions found within this subchapter.

**§ 104.120 [Amended]**

■ 20. Amend § 104.120(a) introductory text by removing the words '', on or before July 1, 2004,''.

**§ 104.200 [Amended]**

■ 21. 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 ''§ 101.550(a) of this subchapter''.

**§ 104.215 [Amended]**

■ 22. Amend § 104.215 as follows:

■ a. In paragraph (b)(5), remove the second use of the word ''and'';

■ b. In paragraph (b)(6), remove the symbol ''.'' and add, in its place, the word ''; and''; and

■ c. In paragraph (b)(7), after the word ''TWIC'', add the symbol ''.''.

■ 23. Amend § 104.235 as follows:

■ a. In paragraph (b)(7), remove the second use of the word ''and'';

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

■ c. Add paragraph (b)(9); and

■ d. Revise paragraph (c).

The addition and revision read as follows:

**§ 104.235 Vessel recordkeeping requirements.**

* * * * *

(b) * * *

(9) *Electronic Reader/Physical Access Control System (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 Canceled Card List with the frequency required in § 101.525 of this subchapter.

(c) Any records required by this part must be protected from unauthorized access or disclosure. TWIC reader records and similar records in a PACS are sensitive security information and must be protected in accordance with 49 CFR part 1520.

**§ 104.260 [Amended]**

■ 24. Amend § 104.260(b) by removing the word ''shall'' wherever it appears

and adding in its place the word ''must''.

■ 25. Add § 104.263 to read as follows:

**§ 104.263 Risk Group classifications for vessels.**

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

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

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

(3) Any vessel engaged in towing a vessel subject to paragraph (a)(1) or (a)(2) of this section.

(b) 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 Vessel Security Plan, 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 moving from a lower Risk Group to a higher Risk Group.

■ 26. Amend § 104.265 as follows:

■ a. Revise paragraph (a)(4);

■ b. Remove paragraphs (c) and (d);

■ c. Redesignate paragraphs (e) through (h) as (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), remove the symbol ''.'' and add, in its place, the word ''; or'';

■ g. Add paragraph (e)(8);

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

■ i. In newly redesignated paragraph (f)(10), 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. Individuals seeking unescorted access to a secure area on a vessel in Risk Group A must pass electronic TWIC inspection and those seeking unescorted access to a secure area on a vessel not in Risk Group A must pass either electronic TWIC inspection or visual TWIC inspection.

* * * * *

(d) * * *

(1) Implement a TWIC Program as set out in subpart E of part 101 of this subchapter, as applicable, and in accordance with the vessel's assigned Risk Group, as set out in § 104.263;

* * * * *

(e) * * *

(8) Implementing additional electronic TWIC inspection requirements, as required by § 104.263, and by subpart E of part 101 of this subchapter, if relevant.

* * * * *

(f) * * *

(11) Implementing additional electronic TWIC inspection requirements, as required by § 104.263, and by subchapter E of part 101 of this subchapter, if relevant.

**§ 104.267 [Amended]**

■ 27. Amend § 104.267(a) by removing the last sentence.

**§ 104.292 [Amended]**

■ 28. Amend § 104.292 as follows:

■ a. In paragraph (b) introductory text, remove the words ''§ 104.265(f)(2), (f)(4), and (f)(9)'' and add, in their place, the words ''§ 104.265(d)(2), (d)(4), and (d)(9)'', and remove the symbol '':'' and add, in its place, the symbol ''—'';

■ 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)''.

■ 29. Amend § 104.405 as follows:

■ a. Revise paragraph (a)(10); and

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

The revision reads 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;

* * * * *

**§ 104.410 [Amended]**

■ 30. Amend § 104.410 as follows:

■ a. In paragraph (a) introductory text, remove the words ''on or before December 31, 2003,'', and remove the symbol '':'' and add, in its place, the symbol ''—'';

■ b. In paragraph (b), remove the words ''or by December 31, 2003, whichever is later''; and

■ c. In paragraph (c) introductory text, remove the symbol '':'' and add, in its place, the symbol ''—''.

## PART 105—MARITIME SECURITY: FACILITIES

■ 31. 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.

■ 32. Revise § 105.110 to read as follows:

**§ 105.110 Exemptions.**

(a) 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 subpart E of part 101 of this subchapter, as applicable, in §§ 105.255 and § 105.285(a)(1).

(b) An owner or operator of any general shipyard facility as defined in § 101.105 of this subchapter is exempt from the requirements of this part unless the facility—

(1) Is subject to parts 126, 127, or 154 of this chapter; or

(2) Provides any other service to vessels subject to part 104 of this subchapter not related to construction, repair, rehabilitation, refurbishment, or rebuilding.

(c) *Public access facility.* (1) The COTP may exempt a public access facility from the requirements of this part, including establishing conditions for which such an exemption is granted, to ensure that adequate security is maintained.

(2) The owner or operator of any public access facility exempted under this section must—

(i) Comply with any COTP conditions for the exemption; and

(ii) Ensure that the cognizant COTP has the appropriate information for contacting the individual with security responsibilities for the public access facility at all times.

(3) The cognizant COTP may withdraw the exemption for a public access facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the exemption or any measure ordered by the COTP pursuant to existing COTP authority.

(d) An owner or operator of a facility is not subject to this part if the facility receives only vessels to be laid-up, dismantled, or otherwise placed out of commission provided that the vessels are not carrying and do not receive cargo or passengers at that facility.

(e) Barge fleeting facilities without shore side access are exempt from the requirements in 33 CFR 101.535(b)(1).

■ 33. Revise § 105.115 to read as follows:

**§ 105.115 Compliance dates.**

(a) Facility owners or operators must submit to the cognizant Captain of the Port (COTP) for each facility—

(1) The Facility Security Plan (FSP) described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) Facility owners or operators wishing to designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure area(s) must do so by submitting an amendment to their FSP to their cognizant COTP, in accordance with § 105.415.

(c) By August 23, 2018, owners and operators of facilities subject to this part must amend their FSPs to indicate how they will implement the TWIC requirements in this subchapter. By August 23, 2018, owners and operators of facilities subject to this part must be operating in accordance with the TWIC provisions found within this subchapter.

**§ 105.120 [Amended]**

■ 34. Amend the introductory text of § 105.120 by removing the words '', on or before July 1, 2004,''.

**§ 105.200 [Amended]**

■ 35. Amend § 105.200 as follows:

■ a. In paragraph (b) introductory text, remove the symbol '':'' and add, in its place, the symbol ''—'';

■ b. In paragraph (b)(6), remove the word ''program'' and add, in its place, the word ''Program'', and remove the word ''part'' and add, in its place, the word ''subchapter'', and remove the symbol '':'' and add, in its place, the symbol ''—'';

■ c. In paragraph (b)(15), remove the words ''section 105.255(c) of this part'' and add, in their place, the words ''§ 101.550 of this subchapter''; and

■ d. In paragraph (b)(16), remove the words ''of this part''.

■ 36. Amend § 105.225 as follows:

■ a. In paragraph (b)(7), remove the second use of the word ''and'';

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

■ c. Add paragraph (b)(9); and

■ d. Revise paragraph (c).

The addition and revision read as follows:

**§ 105.225 Facility recordkeeping requirements.**

* * * * *

(b) * * *

(9) *TWIC Reader/Physical Access Control System (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 Canceled Card List with the frequency required in § 101.525 of this subchapter.

(c) Any record required by this part must be protected from unauthorized access or disclosure. Electronic reader records and similar records in a PACS are sensitive security information and must be protected in accordance with 49 CFR part 1520.

■ 37. 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 or receive vessels carrying CDC in bulk.

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

(b) 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.

■ 38. Amend § 105.255 as follows:

■ a. Revise paragraph (a)(4);

■ b. Remove paragraphs (c) and (d);

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

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

■ e. In newly redesignated paragraph (d)(4) introductory text, remove the word ''shall'' and add, in its place, the word ''must'';

■ f. In newly redesignated paragraph (d)(4)(vi), remove the words ''paragraph (d) of this section'' and add, in their place, the words ''subpart E of part 101 of this subchapter'';

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

■ h. In newly redesignated paragraph (e)(7), remove the symbol ''.'' and add, in its place, the word ''; or'';

■ i. Add paragraph (e)(8);

■ j. In newly redesignated paragraph (f)(8), remove the word ''or'';

■ k. In newly redesignated paragraph (f)(9), remove the symbol ''.'' and add, in its place, the word ''; or''; and

■ l. Add paragraph (f)(10).

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. Individuals seeking unescorted access to a secure area in a facility in Risk Group A must pass electronic TWIC inspection and those seeking unescorted access to a secure area in a facility not in Risk Group A must pass either electronic TWIC inspection or visual TWIC inspection.

* * * * *

(d) * * *

(1) Implement a TWIC Program as set out in subpart E of part 101 of this subchapter, as applicable, and in accordance with the facility's assigned Risk Group, as set out in § 105.253.

* * * * *

(e) * * *

(8) Implementing additional electronic TWIC inspection requirements, as required by § 105.253, and by subpart E of part 101 of this subchapter, if relevant.

* * * * *

(f) * * *

(10) Implementing additional electronic TWIC inspection requirements, as required by § 105.253, and by subchapter E of part 101 of this subchapter, if relevant.

**§ 105.257 [Amended]**

■ 39. Amend § 105.257(a) by removing the last sentence.

**§ 105.290 [Amended]**

■ 40. Amend § 105.290(b) by removing the word ''shall'' and adding, in its place, the word ''must'', and by removing the words ''this part'' and adding, in their place, the words ''subpart E of part 101 of this subchapter''.

**§ 105.296 [Amended]**

■ 41. Amend § 105.296(a)(4) by removing the words ''§ 105.255 of this part'' and adding, in their place, the words ''subpart E of part 101 of this subchapter, as applicable, and in accordance with the facility's assigned Risk Group, as described in § 105.253''.

■ 42. Amend § 105.405 as follows:

■ a. Revise paragraph (a)(10); and

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

The revision reads 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;

* * * * *

**§ 105.410 [Amended]**

■ 43. Amend § 105.410 as follows:

■ a. In paragraph (a) introductory text, remove the words ''On or before December 31, 2003, the'' and add, in their place, the word ''The''; and

■ b. In paragraph (b), remove the words ''or by December 31, 2003, whichever is later''.

## PART 106—MARINE SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

■ 44. 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.

■ 45. Revise § 106.110 to read as follows:

**§ 106.110 Compliance dates.**

(a) OCS facility owners or operators must submit to the cognizant District Commander for each OCS facility—

(1) The Facility Security Plan described in subpart D of this part for review and approval; or

(2) If intending to operate under an approved Alternative Security Program, a letter signed by the OCS facility owner or operator stating which approved Alternative Security Program the owner or operator intends to use.

(b) OCS facilities built on or after July 1, 2004 must submit a Facility Security Plan for approval 60 days prior to beginning operations.

**§ 106.115 [Amended]**

■ 46. Amend the introductory text of § 106.115 by removing the words ''before July 1, 2004,''.

**§ 106.200 [Amended]**

■ 47. Amend § 106.200 as follows:

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

■ b. In paragraph (b)(8), remove the word ''Level'' wherever it appears and add, in each place, the word ''level'';

■ c. In paragraph (b)(9), after the word ''with'', add the words ''the requirements in''; and

■ d. In paragraph (b)(12), remove the words ''§ 106.260(c) of this part'' and add, in their place, the words ''§ 101.550 of this subchapter''.

■ 48. Add § 106.258 to read as follows:

**§ 106.258 Risk Group classification for OCS facilities.**

For the purposes of this subchapter, no OCS facilities are considered Risk Group A.

■ 49. Amend § 106.260 as follows:

■ a. Remove paragraphs (c) and (d);

■ b. Redesignate paragraphs (e) through (h) as (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), 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), 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 subpart E of part 101 of this subchapter and in accordance with the OCS facility's assigned Risk Group, as set out in § 106.258.

* * * * *

(e) * * *

(5) Implementing additional electronic TWIC inspection requirements, as required by § 106.258, and by subpart E of part 101 of this subchapter.

(f) * * *

(9) Implementing additional electronic TWIC inspection requirements, as required by § 106.258, and by subpart E of part 101 of this subchapter.

**§ 106.262 [Amended]**

■ 50. Amend § 106.262(a) by removing the last sentence.

■ 51. Amend § 106.405 as follows:

■ a. Revise paragraph (a)(10); and

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

The revision reads as follows:

**§ 106.405 Format and content of the Facility Security Plan (FSP).**

(a) * * *

(10) Security measures for access control, including the OCS facility's TWIC Program;

* * * * *

**§ 106.410 [Amended]**

■ 52. Amend § 106.410 as follows:

■ a. In paragraph (a) introductory text, remove the words ''On or before December 31, 2003, the'' and add, in their place, the word ''The'' and remove the symbol '':'' and add, in its place, the symbol ''—''; and

■ b. In paragraph (b), remove the words ''or by December 31, 2003, whichever is later''.

Dated: August 8, 2016.

**Paul F. Zukunft,**

*Admiral, Commandant, U.S. Coast Guard.*

[FR Doc. 2016–19383 Filed 8–22–16; 8:45 am]

BILLING CODE 9110–04–P