



# Waves on the Waterfront

CG-FAC, Office of Port and Facility Compliance  
Safety, Security, and Stewardship  
for the Nation's Ports and Facilities

Volume 1  
Issue 2



December  
2012

## BRAVO ZULU!

A special thanks for all who supported and participated at all levels of the Superstorm Sandy MTS Recovery effort. From local MTSRUs and Incident Command staffs, to Area and Headquarters staffs and FEMA liaisons, you provided critical information to the Commandant, the Secretary, and the President, facilitating critical fuel deliveries and the resumption of commerce in some of the areas most devastated by the storm. BZ!

MSU Savannah held a MASFO at five port facilities in Savannah and Brunswick, GA, conducting 107 containerized cargo inspections, 263 vehicle inspections and 371 TWIC checks. The MASFO was performed by 80 officials representing eight agencies and resulted in 75 vehicle and equipment violations, 12 TWIC and license issues with three citations issued, and seven credentials seized.

## ANNOUNCEMENTS

CG-FAC Policy Letter 12-03 was signed on 26 November. This policy clarifies procedures for COTPs to submit annual AMSC reports to CG-FAC. Please, see the article on page 6 for more information!!



Congratulations to CDR Carlos Torres, Chief of the Domestic Ports Division (CG-FAC-1) who will retire on 31 January 2013 after 31 years of faithful and dedicated service!

CDR Torres enlisted in the Coast Guard in January 1982, and after tours of duty in Houston, San Juan and Port Arthur, he attended Officer Candidate School and received a commission in December of 1990.

As an officer, CDR Torres continued his Marine Safety career with assignments to District Seven, MSO Miami, Detachment Supervisor at RIO Borinquen, Chief Inspections Department at MSO Jacksonville, Chief Inspections Department at MSO San Juan, and subsequently Chief Prevention Department at Sector San Juan prior to his current assignment.

A recipient of the Marine Safety Insignia, he earned



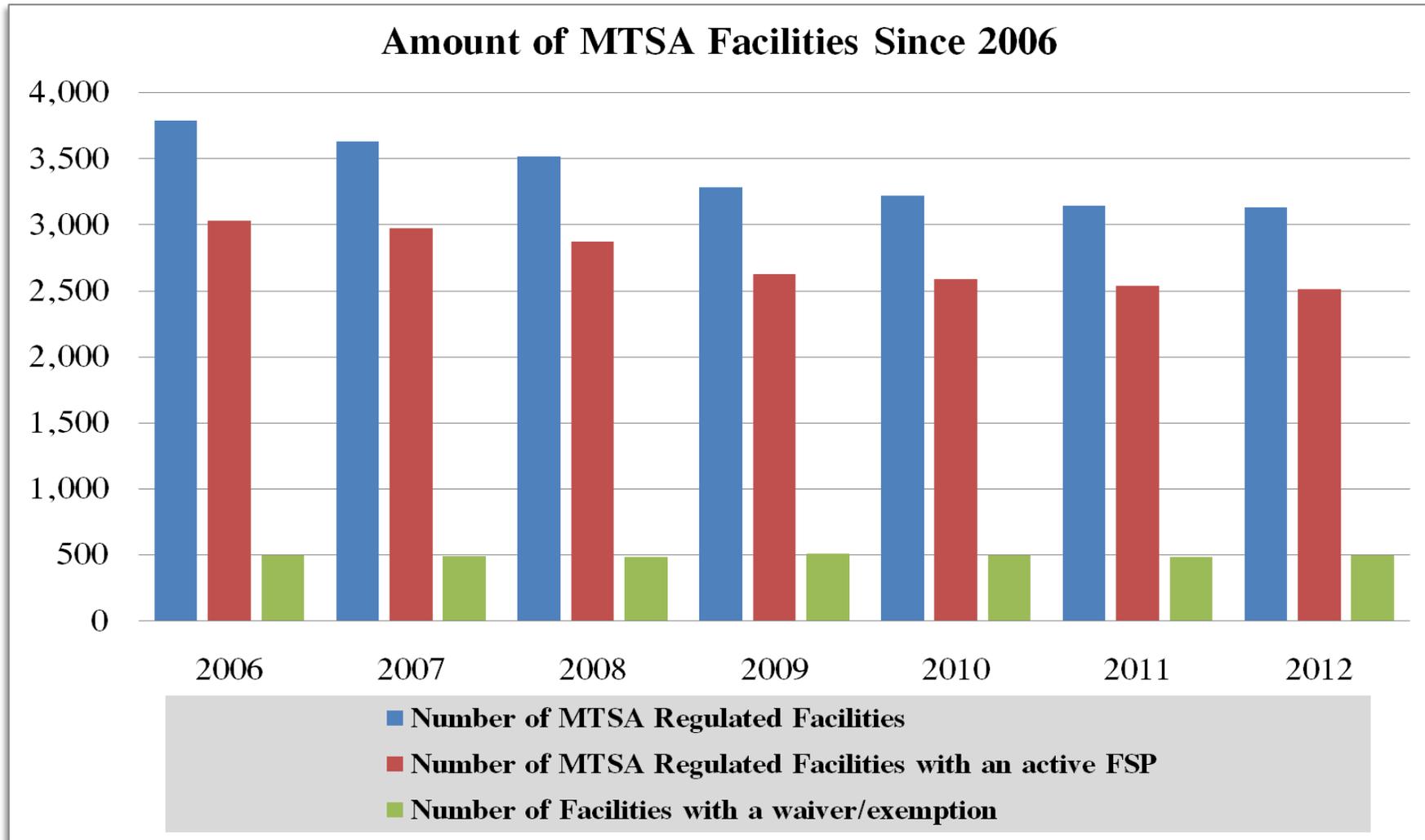
qualifications in Pollution and Violation Investigations, as well as Foreign Freight, Chemical/Oil Tank and Passenger Vessel Inspections and Mariner Licensing Evaluations.

A native of Rio Piedras, Puerto Rico, CDR Torres is a 1980 graduate of the University of Puerto Rico with a Bachelors Degree in Psychology, and has a Masters Degree in Homeland Security from American Military University.

## Next Issue....

- ◆ Meet LT Matt Layman
- ◆ MTS Recovery (CART 2.0)
- ◆ MTSA Breach of Security, Clarified!
- ◆ Public Meeting Report: FSO Training Requirements
- ◆ Updates on EHC National Strategy and Implementation Plan

# Total Safety and Security Facility Populations for Calendar Year 2006 thru 2012



Data retrieved from the USCG Business Intelligence system (CUBEs). The Coast Guard does not track all of the reasons why facilities are no longer MTSA regulated. However, a likely reason for the decrease may be due to economic challenges that forced some facilities to stop activities that would have required regulation under MTSA. The number of MTSA regulated facilities will continue to change due to new facilities coming online, facility closures or operational changes, or the adoption of new rules that change the applicability requirements of the MTSA.

# Secure vs. Restricted Areas, the Mystery Continues...

By Betty McMenemy

Before implementation of the TWIC Program, the term “secure area” wasn’t used as it is today with regards to a waterfront facility. The entire facility was an “access controlled” area and signs had to be *conspicuously* posted stating that “entering the facility is deemed valid consent to screening or inspection; and failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter.” (33 CFR 105.255(f)(3))

Pretty straight forward. Visitors would be screened in accordance with the facility’s approved FSP and enter the facility. No problem.

Then came TWIC and with it, “secure areas” were born.

Basically, a *Secure Area* is an area at a facility over which the owner/operator has implemented access control. This secure area is often referred to as the facility’s ‘footprint.’ Anyone who wishes to gain unescorted/unmonitored access to a secure area must be in possession of a valid TWIC.

A *restricted area* is a part of the infrastructure or a location identified in the facility’s security assessment or by the owner/operator that requires limited access and a higher degree of security protection. Restricted areas of a vessel or facility present a heightened opportunity for a TSI. It’s very easy to determine secure vs. restricted on cargo ships: the entire vessel is a secure area and access control measures are in place to keep unauthorized persons from gaining access to the vessel. On-board the vessel are other areas that require a higher degree of security – e.g., the pilot house and the engine room. These areas ARE restricted areas that lie WITHIN a secure area and do require a valid TWIC for unescorted access.

Facilities are not quite so straight forward. Many facilities are surrounded by a fence. Therefore, with the advent of TWIC, the entire fenced in area became a secure area – and required a TWIC for unescorted/unmonitored access. However, what about facilities with parking lots inside their fence? This means access to the parking lot requires a TWIC! What about visitors?

What about administrative personnel who have no involvement in the maritime portion of the facility?

NVIC 03-07 discusses how facilities may redefine their secure areas to include only those

portions of the facility that are involved in maritime activities. Certain facilities can benefit greatly from this redefinition: factories, mills, refineries, etc. Redefining a facility’s footprint can greatly reduce the area that requires access control measures therefore reducing the number of facility personnel that require TWICs.

The final footprint or secure area of a facility has access control, and a TWIC is required in order to gain unescorted/unmonitored access. A non-TWIC holder needing access to a secure area must be accompanied or, in some cases, monitored.

*Monitoring* means the ability to sufficiently observe an individual so as to be able to respond if they are observed engaging in unauthorized activities or entering an unauthorized area.

Although a facility may declare the entire footprint as restricted, not many facilities operate this way. There are two types of restricted areas: those that are *inside* a secure area and those that may be *outside* of a secure area. Let’s take a look at the illustration below for a better understanding.

This green rectangle represents the facility’s footprint, the *secure area*.

Restricted area *within* a secure area

This pink oval is a restricted area within a secure area.

Located 300 yards behind the facility is a small brick building which houses a backup generator. This *is* a restricted area but it is *NOT* located within a secure area. This area *does NOT require a TWIC* for unescorted access but all of the requirements found in 33 CFR 105.260 (Security measures for restricted areas) *must* be applied to this restricted area.

Location of back-up generator. A restricted area *outside* of a secure area.

The entire rectangular area is the “secure” area of the facility and unescorted/unmonitored access requires a TWIC.

The “oval” shape located *within* the secure area of the facility represents the location of security and surveillance equipment and systems, etc. This is a restricted area and requires a TWIC for unescorted access *because it is within a secure area*.

Mystery solved. Still have questions? Let us know, we’re always happy to help.

# Details on the EED TWIC!

by LT Matthew Layman

In order to comply with the new federal regulations, MTSA facilities began implementing and enforcing TWIC requirements during the Spring of 2009. Leading up to this period, a diverse influx of transportation workers applied for and received TWICs throughout CY 2008.

As we quickly approach CY 2013, a significant number of these TWICs will begin expiring. Consequently, TSA expects to receive a flood of TWIC renewal applications over the next 2 years. In fact, one month after announcing the Extended Expiration Date (EED) TWIC, TSA released a statement stating that TWIC call centers were already overwhelmed with the number of EED applications.

In response, TSA requested TWIC holders wait until they were within 4 months of their expiration date before renewing their credential, at least until TSA could increase call center capacity. Needless to say, there is concern throughout industry that TWIC renewal efforts will continue to



bottle neck and, as a result, facilities will find themselves in a situation where their workforce is stuck outside the gates.

The following Q's & A's highlight many of the common questions fielded daily by the CGHQ TWIC Help Desk and are provided to help clarify several program policies.

**What should be done when someone tries to gain access to an MTSA facility with an expired TWIC--besides denying access--is there anything else the facility should do to prevent the individual from trying to access another facility?**

An individual presenting an expired TWIC should be denied access to the facility or should be escorted as if they do not have a TWIC. If all facilities conduct the prescribed visual check of the card, there should be no concern over the individual gaining access to another facility.

**Does use of an expired TWIC constitute a potential or reportable suspicious activity and/or breach of security and does this need to be reported to NRC?**

Presenting an expired card alone (aside from any other suspicious activity) should not necessarily raise immediate concern; the person simply let their card expire for which there can be many reasons. If there is additional information that raises the level of suspicion, then the case should be treated appropriately.

**Can an employer confiscate an individual's TWIC?**

Per the Code of Federal Regulations 49 CFR 1572.19(c), the TWIC is the property of the Transportation Security Administration (TSA), and held by the individual to whom the card was issued. The TWIC allows an individual worker to gain employment with any company that requires access to secure areas within a MTSA facility, and should not be taken from the Worker (even if it is damaged, expired, or on the CCL).



Only federal, state, and /or local law enforcement agencies should confiscate TWICs. There is one exception to this standard: an employer must retrieve a TWIC from an alien who is working pursuant to a visa listed in 49 CFR 1572.105(a)(7) when the visa expires or when the work authorized by the visa expires. In this case, the employer must return the TWIC to TSA.

**Will facilities be permitted to grant access to individuals whose TWIC is expired if the individual has a receipt indicating that he/she has ordered a replacement?**

NVIC 03-07 enclosure II and PAC 03-09 change 4 provides guidance on the authority of the Captain of the Port to grant extended temporary access to individuals whose TWIC was lost, stolen, or damaged and have ordered a replacement card. At the discretion of the local COTP, this policy can be extended to include individuals who have an expired TWIC and can demonstrate that they have enrolled and applied for either an EED or Standard 5-year TWIC.

**How does the Canceled Card List compare to Santa's Naughty List?**

Lets put it this way. You don't want to be on either...

There are many more helpful questions and answers available on the TSA [website](#). If you have more questions regarding TWIC, please email us at [TWIC.HQ@uscg.mil](mailto:TWIC.HQ@uscg.mil).

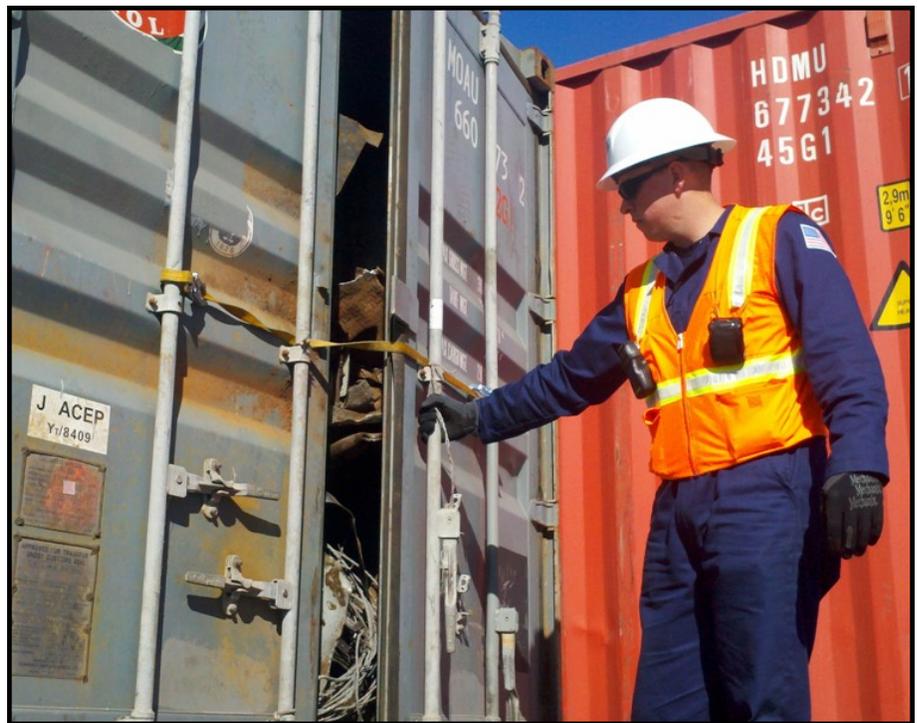


# WE WANT TO HEAR FROM YOU!!!!!!

CG-FAC strives to provide the best possible service and stay informed of challenges and successes in the field. A short voluntary survey is provided at the link below which allows you to submit policy concerns/suggestions, unit developed best practices, and mission successes in a short, easy to use on-line form. Please use your chain of command as appropriate and ensure your comments or concerns are policy related, and not focused on specific operational questions. Widest participation is requested - the more we know, the better service we can provide you! Instructions to submit feedback are contained on the website.

[Click Here!](#)

Thanks to LTJG Heather Lampert of Sector San Francisco for sharing this excellent reminder of the importance of following proper procedures and safe work practices. This photograph shows MK2 Reggie Wellemeyer in the process of conducting a routine container inspection. MK2's commitment to safety ensured he was not hit by the container door or the scrap metal contents trying to escape! Thank you "Safety Strap"!



[Safety may begin with an S, but it's starts with YOU!!!!](#)

## **CG-FAC Policy Letter 12-03: AMSC Annual Reporting Requirements**

**by LTJG Cale Cooper**

In recent months, CG-FAC has worked on a new policy letter for distribution to all Area Maritime Security Committees (AMSC's) nationwide. The policy letter is periodically updated and outlines AMSC reporting and endorsement requirements. This year CG-FAC has added a little twist to the policy letter, not by creating new requirements for the field, but by presenting new practices that CG-FAC will implement at the headquarters' level. CG-FAC will now directly respond back to any AMSC that presented questions or areas of concerns in their annual report. This will close a critical feedback loop between headquarters and the field. In addition to these new procedures, this policy letter update also establishes an "AMSC of the Year" award. The nomination and endorsement procedures to this award are also contained in the policy letter.

To assist in closing this feedback loop with the field, CG-FAC reviewed all annual reports and constructed a matrix form that sorted and categorized questions and areas of concern submitted by the AMSCs. Once organized, the submissions are addressed either directly by CG-FAC or forwarded to the appropriate headquarters element to generate a response to the field. Eventually, the tracking matrix created by CG-FAC will be forwarded via Homeport community announcement and posted to the PSS and AMSC Management communities. This effort will allow various AMSCs to view the status it's own submittals as well as obtain information submitted from or to other committees.

Following the Joint Harbor Safety Committee (HSC) – Area Maritime Security Committee (AMSC) Conference this past August, CG-FAC was inspired to establish an annual AMSC award that would recognize the hard work AMSCs engage in every day to safeguard the many port areas throughout the nation. CG-FAC crafted the general award and nomination requirements and received feedback and concurrence within CG Headquarters as well as from both Areas. The award procedures are provided in the AMSC policy letter update and the nomination requirements are

in sync with the annual reporting requirements schedule. Enclosures are attached to the policy letter to guide Captains of the Port (COTPs) and AMSC's through the nomination process. Once the Districts have prioritized and ranked the AMSC applying for the award, they will forward to CG-FAC for review and subsequent consideration by the "AMSC of the Year" Awards Selection Committee to determine the award recipient. The Awards Selection Committee is composed of one representative from CG-FAC, CG-PSA, CG-MSR, LANT-55, and PAC-54. The winner of the award will be announced via Coast Guard Message System (CGMS) and recognized at the next HSC-AMSC Conference or AMSC specific workshop or conference each year.

If you have questions or feedback relating to the AMSC program, including name-based terrorist checks, security clearances for AMSC members, annual reporting requirements, the newly established "AMSC of the Year" award, AMSC conferences or workshops, or AMSC support funds please contact CG-FAC-1's Port Operations Branch via email at [AMSC@uscg.mil](mailto:AMSC@uscg.mil).



# Sea Partners Campaign

The Sea Partners Campaign is the Coast Guard's environmental education and outreach program. Sea Partners is a pro-active and innovative aspect of the Coast Guard's compliance mission under the Marine Safety and Environmental Protection program and seeks to provide waterways users, such as boaters, fishermen, marina operators, marine industry, and the general public with information on protecting the marine environment.

Sea Partners was originally established in 1994 and remains the only environmental education program in the Coast Guard. During 1997 the Coast Guard expanded the program to the Coast Guard Auxiliary, allowing Auxiliarists to earn a Marine Environmental Educator qualification to prepare them to conduct Sea Partners events. Sea Partners is also the only Coast Guard initiative to meet the Coast Guard's legacy obligations for public education under the Plastic Pollution Research and Control Act of 1987, which directed the Secretary of Transportation (as the department in which the Coast Guard was operating), together with the Adminis-



trator of the National Oceanic and Atmospheric Administration and the Administrator of the Environmental Protection Agency, to commence and conduct a public outreach program to educate the public on environmental protection.

Over the last two decades a wide range of audiences have been targeted by the Sea Partners Campaign, including federal, state, and local officials; merchant mariners; offshore industry personnel; ferry operators; recreational boaters; sport and commercial fishermen; seafood processors; local business owners; marina operators; students; scouts; and the list goes on. Between June 1994 and November 2012, Sea Partners teams, mostly consisting of reservists and Auxiliarists, have dedicated over 93,000 hours to raising public awareness about the importance of environmental protection and stewardship. These teams have reached millions of individuals through personal contact, as well as through print media, radio, and television.

# **Regulatory Projects Update**

by LCDR Loan O'Brien

The Security Standards Branch (SSB) is currently managing several regulatory projects which will impact MTSA-regulated facilities. SSB projects and background info include:

**1. TWIC Reader Requirements Notice of Proposed Rulemaking (NPRM):**

Background: Proposes to require certain vessels and facilities to use electronic readers designed to work with the TWIC.

Status: Rulemaking package was accepted by the Office of Management and Budget as of November 16, 2012.

Timeline for NPRM publication: Anticipate early 2013 with at least two public meetings (locations and dates to be determined).

**2. Consolidated Cruise Ship Security Measures NPRM:**

Background: Proposes to amend existing cruise ship terminal security regulations.

Status: Rulemaking package under review.

Timeline for NPRM publication: Anticipate mid to late 2013 pending further review and approval.

**3. Updates to 33 Code of Federal Regulations Subchapter H (MTSA2) NPRM (aka MTSA II):**

Background: Proposes to amend maritime security regulations to incorporate new statutory and international requirements, policy decisions interpretations, and clarifications of existing regulatory text.

Status: Rulemaking package under development with USCG regulatory team.

Timeline for NPRM publication: Anticipate late 2013 pending further review and approval.

**4. U.S. Coast Guard Authorization Act of 2010 (CGAA) Section 811 - Seafarer Access:**

Background: Proposes to implement a system that ensures mariners and other individuals have access through the facility and between vessels moored at the facility.

Status: Rulemaking package under development with USCG regulatory team.

Timeline for NPRM publication: Anticipate late 2013 pending further review and approval.

**5. CGAA Section 821 - Facility Security Officer Training and Certification:**

Background: Public meeting conducted November 9, 2012; draft model course posted on-line at <https://homeport.uscg.mil/mtsa>.

Status: Public comments being reviewed and adjudicated for model course and policy letter development.

Timeline: Anticipate late 2013 for NPRM pending rulemaking development.

**6. CGAA Section 822 - Integration of Security Plans and Systems:**

Background: Notice and requests for comments from facility owners and operators, State and local law enforcement agencies, port authorities, relevant security industry participants, and all other interested members on implementing this mandate.

Status: Notice and request for comments under development.

Timeline: Anticipate early 2013 pending further review and approval.

Rulemaking projects such as the various NPRMs will publish in the Federal Register (<https://www.federalregister.gov/>). CG-FAC will also post the notices and other relevant information on Homeport. A good article on the Coast Guard's rule-making process is in the Spring 2010 Coast Guard Proceedings magazine (Volume 66, Number 4) at <http://www.uscg.mil/proceedings/spring2010/>.

**Office of Port and Facility Compliance**

Captain Andrew Tucci

202 372-1080

**Domestic Ports (CG-FAC-1)**

CDR Carlos Torres

202-372-1107

Mr. Wayne Young

202-372-1118

**Port Operations (AMSC & MTS Recovery)**

LCDR Dwayne Meekins

202-372-1106

LT Brad Bergan

202-372-1149

**Information & Industry Outreach (NMSAC)**

Mr. Ryan Owens

202-372-1108

LCDR Ulysses Mullins

202-372-1106

**Cargo and Facilities (CG-FAC-2)**

CDR Jeff Morgan

202-372-1171

Mr. Jim Bull

202-372-1144

**Security Standards (Regulation Development)**

LCDR Loan O'Brien

202-372-1133

LCDR Jose Ramirez

202-372-1131

**Cargo & Facility Security (MTSA)**

LCDR Kevin Floyd

202-372-1132

LT Russell Amacher

202-372-1131

**TWIC Implementation**

LCDR Gregory Callaghan

202-372-1168

LT Matthew Layman

202-372-1160

**Facility Safety & Outer Continental Shelf**

LCDR Kevin Lynn

202-372-1130

Mr. David Condino

202-372-1145

LT Mike St. Louis

202-372-1114

MSTC Kevin Collins

202-372-1127

**USCG TWIC Help Desk**

202-372-1166

[TWIC.HQ@uscg.mil](mailto:TWIC.HQ@uscg.mil)