DEPARTMENT OF HOMELAND SECURITY

UNITED STATES COAST GUARD

OFFICE OF PORT AND FACILITY COMPLIANCE

2016 ANNUAL REPORT

Table of Contents

CG-FAC Policy Review

Throughout this document, various policies, instructions, and strategies are referenced. For a comprehensive list and electronic access to these documents, please see the CG-FAC links at the back. Please note: some of these items may require Coast Guard access to the CG-only web Portal.

On the Front Cover
Virginia Port Authority's Portsmouth Marine Terminal.

INTRODUCTION

The mission of the Office of Port and Facility Compliance (CG-FAC) is to provide Safety, Security, and Stewardship for the Nation's Ports and Facilities. CG-FAC strives to provide clear regulations, policy and direction to Coast Guard Operational Commanders and other stakeholders to ensure our ports communities are a safe, secure place to do business, live, and work.

CG-FAC continues to be on the forefront of developing guidance to address a myriad of new technologies and risks in the maritime community. Dependence on cyber systems and the need to ensure their security was a dominate focus on FAC's work this past year. Working with the Department of Transportation and Transportation Security Administration, CG-FAC developed Enhanced Coordination Procedures (ECPs) as outlined in Presidential Policy Directive 41 (PPD -41), titled "United States Cyber Incident Coordination." ECPs are designed to enhance unity of effort and ensure consistent response procedures are developed, deployed, and updated as appropriate. CG-FAC also provide significant programmatic support to the creation of the Office of Cyberspace Forces (CG-791), and worked with NIST to finalize a Cybersecurity Framework Profile for Maritime Bulk Liquid Transfer facilities.

CG-FAC championed efforts for a service level agreement (SLA) between the Coast Guard, National Response Center and DHS' National Cybersecurity and Communications Integration Center (NCCIC) to coordinate reporting of cyber related events. This was integral in the recently released Commandant Instruction Manual and CG-5P Policy Letter 08-16, which outlines the criteria and process for suspicious activity (SA) and breach of security (BoS) reporting. Coast Guard Captains of the Port, Area Maritime Security Committees and the operators of vessels and facilities may use this policy letter when evaluating SA and BoS incidents.

Most importantly, CG-FAC is extremely proud to support the Coast Guard men and women who in 2016, completed nearly 12,000 facility inspections (51% of which were MTSA compliance inspections), over 54,000 visual and electronic inspections of Transportation Worker Identification Credentials, and more than 23,000 container inspections. Maintaining a strong operational presence on the waterfront is key to safe, secure ports. In addition, Port Security Specialists oversaw the coordination of 93 events that tested the effectiveness of their respective port-level AMS Plans and supported maritime security preparedness regimes through the engagement of federal, state, local, tribal, and territorial government and private sector stakeholders. We are equally grateful to the many facility operators, port workers, mariners, and other agency personnel whose patriotism and hard work are equally vital to our success.

Captain Ryan D. Manning, USCG

Highlights of 2016

Common Assessment and Reporting Tool (CART)

CG-FAC-1 continues to manage, monitor, and update the Marine Transportation System Recovery Common Assessment and Reporting Tool (MTSR CART) program to support field personnel with port recovery and status reporting. The MTSR community promoted and received a modification to CART to include new categories of Essential Elements of Information (EEIs) this year. This modification will assist field units in accurately reporting the status of key operations within the port and provide senior leaders with a valid measurement of the health of the port- post incident. New changes to further streamline these revisions are in progress.

FAC Notes

In an effort to increase the flow of communication between the program office and field units, CG-FAC introduced *FAC Notes*, a monthly document consisting of policy updates, best practices, program announcements, and other pertinent information. *FAC Notes* are posted monthly on the CG-FAC-2 CG Portal page. Suggestions and contributions are always welcome!

Office of Cyberspace Forces

CG-FAC provided near full-time programmatic support to the CG-791 Implementation Team (Office of Cyberspace Forces). This program office was created as a result of the one year effort of the Cyber-CIO-C4IT Governance and Transformation Task Force Blueprint. The goal of this program office is to realign the C4ITSC, CG-6, TISCOM, and CG-791 to better address the CG Cyber Strategy and to weave the Cyber Workforce initiatives into the CG Human Capital Plan. CG-FAC will continue collaboration and involvement with the CG-791 program office until fall 2017.

Highlights of 2016

iPad Program

CG-FAC-2 completed the distribution of 120 iPads to Facility Inspection teams throughout the Coast Guard, thereby reducing the need to carry large quantities of references and materials that could weigh nearly 30 - 40 pounds. Facility Inspectors have provided some great feedback on how they are using the iPads, including the use of authorized wireless printers that can be obtained from ITCCB (https://itccb.uscg.mil/ITCCB-Home/default.aspx). Training Center Yorktown, Port Operations School, has also been issued iPads which have been used to replace the references used in the Waterfront Facility Inspector and Explosive Handling Supervisor courses. This initiative has allowed the instructors to demonstrate ways to use the devices, and students to become familiar with them in a training environment. We appreciate continued feedback and will post lessons learned and other tools for the iPads at https://cg.portal.uscg.mil/units/cgfac2/iPads/SitePages/Home.aspx.

Port Security Specialist (PSS) Program

CG-FAC-1, working with Force Readiness Command, the Performance Technology Center (PTC) at Yorktown, Virginia, conducted a Front End Analysis (FEA) for both the PSS & Security Specialist Port/Recovery (SS P/R) workforce. The FEA, referred to as the "analysis", developed a job requirement task list and will help to identify the performance support (e.g. training, Tactics, Techniques, and Procedures (TTP), e-training, job aids) needed for PSS/SS P/R personnel to perform at an optimal level in accordance with the duties and responsibilities as outlined by their position descriptions (PD). CG-FAC is currently entering the pre-design/scoping phase of the New Performance Planning (NPP) cycle (next phase directly after the FEA or analysis phase in the training design process). CG-FAC and PTC Yorktown are currently examining each task to (1) determine if a solution already exists and (2) if not, identify the appropriate solution(s). As a result of this review, CG-FAC's Mr. Bob Reimann is moving ahead with the Design and Scoping phase of a Port Security TTP manual.

CG-FAC had to compete with many other CGHQ offices/projects to be selected for this support. FORCECOM's TTP division will be supporting CG-FAC through this evolution. The scope of these productions, modified from the outline approved by the TTP screening board (FC-P), will focus on how to complete specific tasks required of a PSS. These task specific publications will serve to standardize and improve the completion of specific PSS job tasks throughout the Coast Guard. During the design phase, FC-P staff will assist CG-FAC in identifying other specific tasks for potential development. Addressing the training and performance issues has always been one of CG-FAC's top priorities. This NPP effort will enhance the workforce's credibility within their public and private constituency.

Highlights of 2016

Arctic, Caribbean, and other CG-FAC work on Prevention of Pollution of the Marine Environment:

CG-FAC-2 staff has been working with the NOAA– led US Delegation to the Arctic Council Work Group on Protection of the Arctic Marine Environment (PAME) as routes over the North Polar seas open up. The work group is assessing increases in shipping traffic in the Arctic due to climate change and marine transportation infrastructure at Arctic and near Arctic ports, such as port reception facilities required by MARPOL (Polar Code Amendments came into force on Jan 1, 2017). Proposals are being drafted on ship's waste management and pollution prevention in Arctic waters for Arctic countries to take to MEPC through their IMO Delegations.

CG-FAC-2 has been working with US trading partners in the Wider Caribbean Region, as part of United Nations Environmental Program/International Maritime Organization (IMO) initiatives to provide technical assistance, education, and outreach on MARPOL compliance and regional approaches to ship's waste management. In October 2016, a workshop in Trinidad & Tobago produced a plan to move forward with regional waste management approaches and cooperation among Wider Caribbean small island developing states in the region.

CG-FAC-2 staff represents the American National Standards Institute at the International Organization for Standardization (ISO), based in Geneva, in efforts to develop international standards for operation of ships and for the protection of the marine environment. Two existing ISO standards for the management of ship's waste have been recently revised, due to changes in MARPOL, and are currently in the final stages of publication.

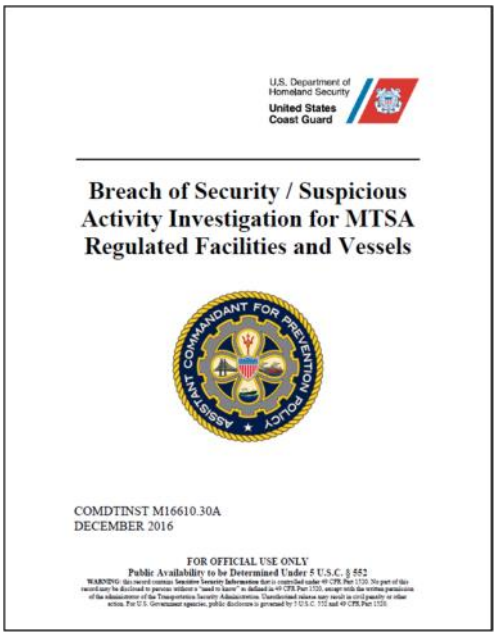
Coast Guard LNG Workgroup

CG-FAC continues to chair the Coast Guard's Liquefied Natural Gas (LNG) Workgroup and during this last year provided program oversight and expertise with the development of numerous field notices issued by the Liquefied Gas Carrier National Center of Expertise. These field notices allowed the consistent application of regulations and nationwide policy as the marine industry continues to expand its use of LNG as a fuel and provided an outline for what the industry and Coast Guard should consider when developing and approving safe simultaneous operations when bunking vessels using LNG as a fuel.

Highlights of 2016

Updated Breach of Security & Suspicious Activity Reporting Procedures

CG-FAC published COMDTINST 16610.30A (FOUO) and CG-5P Policy Letter 08-16, which outlines the criteria and process for suspicious activity (SA) and breach of security (BoS) reporting. Coast Guard Captains of the Port, Area Maritime Security Committees and the operators of vessels and facilities regulated by the MTSA may use this policy letter when evaluating SA and BoS incidents. This policy letter also covers reporting requirements and guidance on reporting cybersecurity related events.


U.S. Department of Homeland Security
United States Coast Guard

Breach of Security / Suspicious Activity Investigation for MTSA Regulated Facilities and Vessels

ASSISTANT COMMANDANT FOR PREVENTION POLICY

COMDTINST M16610.30A
DECEMBER 2016

FOR OFFICIAL USE ONLY
Public Availability to be Determined Under 5 U.S.C. § 552

Cyber incidents are unique and inherently complex and require a specific skill set to be properly documented. As a result, the Department of Homeland Security (DHS) National Cyber Security and Communications Integration Center (NCCIC) may be contacted directly for cybersecurity incidents and suspicious cyber activity not resulting in physical or pollution effects (incidents resulting in physical or pollution effects must be reported to the National Response Center (NRC).

When contacting the NCCIC, maritime owners/operators must identify themselves as a MTSA regulated entity in order to satisfy the reporting requirements of 33 CFR 101.305. The NCCIC documents the report, evaluates it against current operations, provides technical assistance if requested and appropriate, and passes the collected information to the NRC. Information sharing between NCCIC and the NRC may contain sensitive security information and is protected in accordance with 49 CFR 1520. COMDTINST 16610.30A is FOUO and is available in Directives on CG Portal. The CG-5P Policy Letter 08-16 is available by electronic means only by accessing: https://Homeport.uscg.mil (select “maritime security” link and look under the policy section). Questions or comments with respect to this policy can be e-mailed to: CGFAC@uscg.mil

Cyber Risk Management

Since the signing of the Cyber Strategy, CG-FAC remains the lead office for implementing the Protect Infrastructure portion of the Strategy. The Protect Infrastructure Cyber Strategy Implementation Team (CSIT) remains committed to accomplishing the goals set forth in the Cyber Strategy. The representatives from CG-5P, CG-2, CG-6, CG-5R, National Maritime Center (NMC), Areas and Districts collaborate to achieve significant program level milestones. One such milestone was the completion of the draft Cyber Navigation Vessel Inspection Circular that is anticipated to be released via the Federal Register in spring of 2017 for public comment.

PPD-41

CG-FAC, working with the Department of Transportation and Transportation Security Administration, developed Enhanced Coordination Procedures (ECPs) in accordance with directives outlined in Presidential Policy Directive 41 (PPD-41), titled "United States Cyber Incident Coordination." PPD-41 was published on July 26, 2016 and defines what constitutes a significant cyber incident and more importantly, who is responsible for responding to a significant cyber incident. ECPs are designed to enhance unity of effort and ensure that consistent response procedures are developed, deployed, and updated as appropriate.

MBLT

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CG-FAC, working with the NIST and maritime industry stakeholders, developed the voluntary Cybersecurity Framework Profile (CFP) for the Maritime Bulk Liquid Transfer (MBLT) facilities and released them in November 2016. The MBLT CFP serves to assist in cybersecurity risk assessments for those entities involved in MBLT operations as overseen by the USCG. It is intended to act as non-mandatory guidance to organizations conducting MBLT operations within facilities and vessels under the regulatory control of the USCG under the Code of Federal Regulations (CFR) 33 CFR 154-156.

2016 Facility Inspections Program Statistics

Total regulated facilities:	
MTSA-regulated facilities	***3,476***
Facilities with Safety Regulations (exempted from MTSA)	***1,678***
Total facility inspection activities completed:	**11,856**
MTSA facility inspection activities completed:	***6,002***
Total container inspections completed:	**23,809**
Total transfer monitors conducted:	**666**
Total operational controls (COTP Orders):	**41**
Security COTP Orders	***6***
Safety/Environmental Protection COTP Orders	***35***

2016 MTSA Security Compliance by District

District	FSPs*	MTSA Inspections	Deficiencies
1st	287	792	168
5th	165	419	146
7th	296	682	241
8th	885	2,270	577
9th	302	705	171
11th	138	450	108
13th	139	314	147
14th	74	157	66
17th	97	213	24
Total	**2,383**	**6,002**	**1,648**

**: Number of facilities within each district required to maintain USCG-approved Facility Security Plans.*

2016 MTSA Facility Enforcement Actions

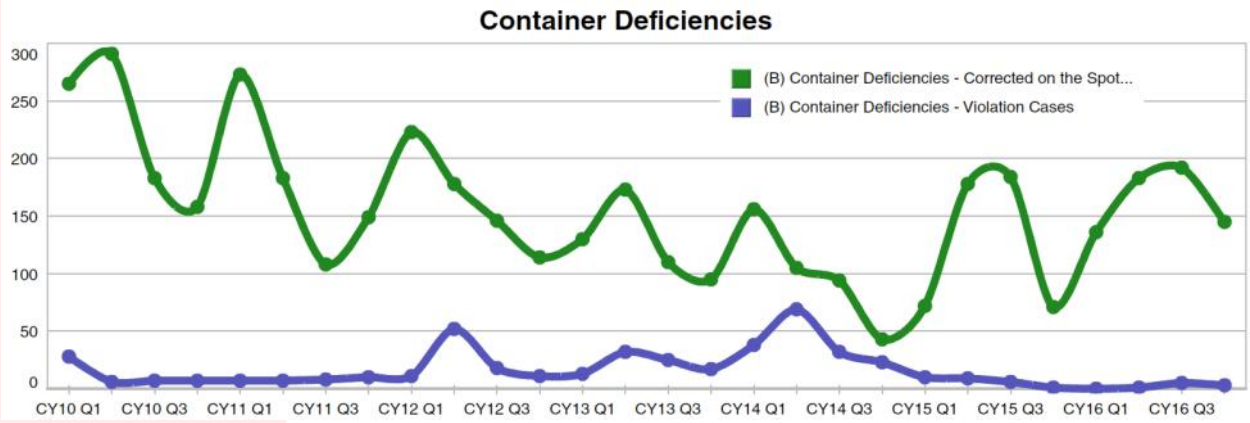
In 2016, the Coast Guard completed 6,002 security-related MTSA annual and spot check examination activities and recorded 180 enforcement activities against MTSA-regulated facility owners or operators for noncompliance with MTSA regulations. In some cases, examinations of a facility were not conducted due to the facility closing or changing their operations, thus removing them from Coast Guard oversight. The 180 enforcement activities executed in 2016 took place at 115 MTSA-regulated facilities and included letters of warning or administrative civil penalties.

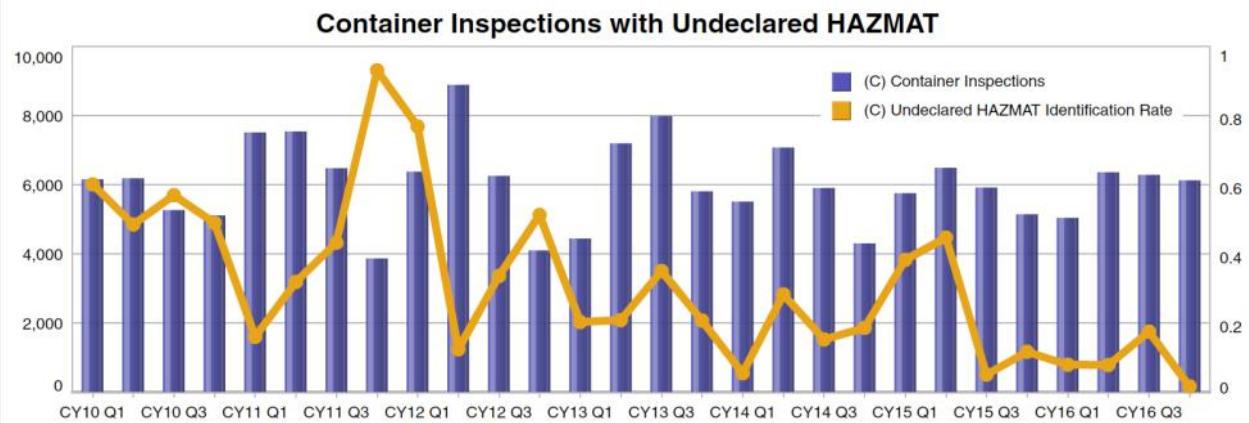
Citation	Citation Title	Enforcement Activities Executed
33 CFR 101.305	Reporting, Breach of Security	5
33 CFR 105.125	Noncompliance	3
33 CFR 105.140	Alternative Security Program	1
33 CFR 105.200	Owner or operator requirements	32
33 CFR 105.205	Facility Security Officer requirements	12
33 CFR 105.210	Facility personnel with security duties	9
33 CFR 105.220	Drill and exercise requirements	17
33 CFR 105.225	Facility recordkeeping requirements	6
33 CFR 105.255	Security measures for access control	61
33 CFR 105.260	Security measures for restricted areas	10
33 CFR 105.275	Security measures for monitoring	4
33 CFR 105.290	Additional cruise ship terminal requirements	0
33 CFR 105.305	Requirements for facility security assessments	0
33 CFR 105.400	Facility Security Plans	5
33 CFR 105.410	Facility Security Plans – Submission and approval	5
33 CFR 105.415	Facility Security Plans – Amendment and audit	10
Total		**180**

Container Updates

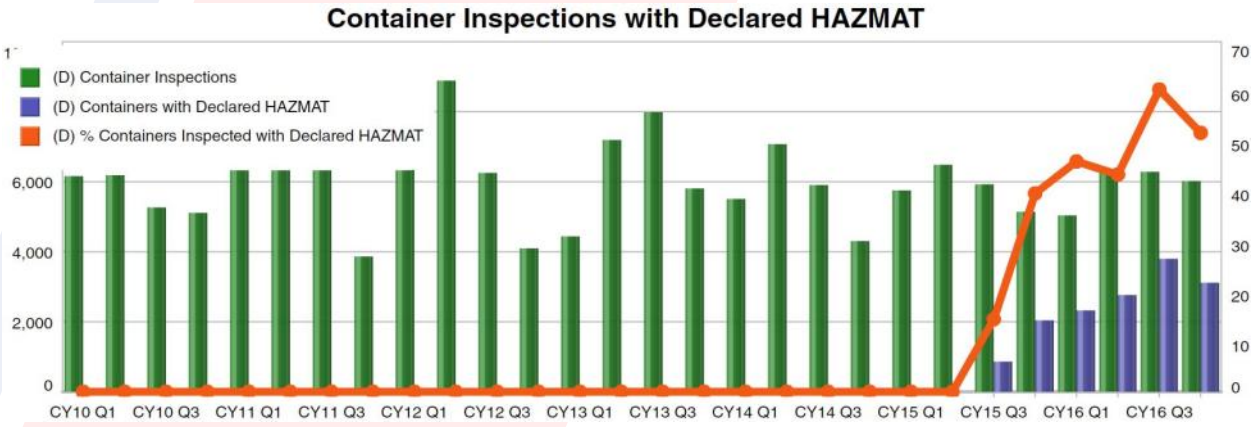
CG-FAC continuously seeks to improve the National Container Inspection Program (NCIP) guidance and streamline the process for both industry and the field. CG-FAC recently met with Hapag-Lloyd and the National Cargo Bureau to discuss industry and Coast Guard concerns and issues with the shipment of containers in an effort to identify ways we can work together to mitigate risks. To that end, Hapag-Lloyd has developed a system called "Watchdog" that analyzes shipping documents searching for key words to assist in selecting containers for inspection. Watchdog has enabled Hapag-Lloyd to inspect 20% of all containers shipped by the company. Industry's proactive measures and initiatives, such as Watchdog, continue to lead to higher compliance rates and have shed light on what problems or issues are still occurring.

Mis-declared cargo and leakage are the most prominent issues seen in the shipment of containers and account for 86% of deficiencies recorded by the Cargo Incident Notification System website. According to the same website, over 70% of those deficiencies involve general cargo shipments, which point to the success of inspection programs focused on declared Hazardous Materials (HAZMAT).





Container Updates



The Coast Guard conducts three types of containers inspections: Declared, General and Structural. "Declared" inspection refers to containers with declared hazardous materials and includes such things as verifying paperwork and packaging requirements. "General" inspections contribute to identifying shipments of un-declared HAZMAT or other deficiencies with a container. "Structural" inspections occur during every container inspection and help ensure the structural serviceability of containers. Containers with structural damage can cause or contribute to significant safety risks to the vessels, facilities, and the personnel working with or around them.

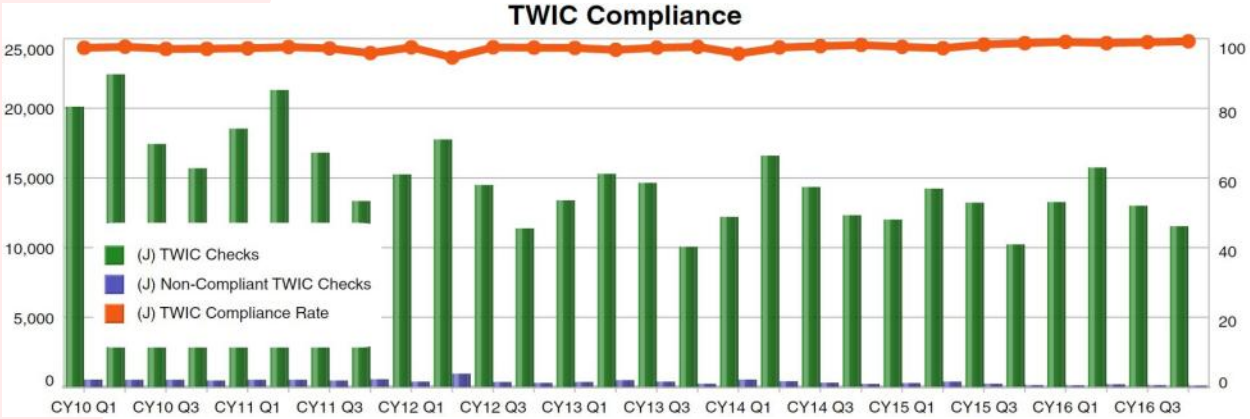
Higher national compliance rates in declared HAZMAT shipments led to a shift for inspections rates of declared HAZMAT and general cargo container shipments. Previous guidance prioritized HAZMAT over general cargo shipments at a 90% to 10% inspection goal respectively. On average, of the total containers inspected nationally, the Coast Guard has achieved roughly 60% to 40% HAZMAT to general cargo annually.

The new 50/50 model is an interim change to better identify all potential or existing risks in all types of containerized cargo shipments. CG-FAC will continue to monitor inspection results and data to update the program and the field as needed. Input from the field is always welcomed and appreciated as we continue to improve the NCIP to reduce risk and improve safety both at sea and ashore.

Transportation Worker Identification Credential (TWIC) Verifications

As part of the MTSA security program, Facility Inspectors conducted a combined 54,166 visual and/or electronic inspections of TWIC cards in 2016 and identified 515 instances of non-compliance with TWIC requirements. Electronic TWIC inspections are an important component of the Coast Guard's layered maritime security and CG-FAC encourages field units to continue using the deployed readers during each inspection, combined with visual card verifications. CG-FAC has a service contract in place to support technical/operational issues for the hand-held readers as they approach their end of service life. Please contact CG-FAC to take advantage of that support. CG-FAC is currently conducting market research for replacement readers. We anticipate purchasing replacements in conjunction with implementation of the TWIC reader final rule in order to ensure that the Coast Guard's electronic readers are in compliance with what is required of our stakeholders. As an example, there are currently a few units conducting field testing for iPad based reader applications. These initial tests have been successful to date and may be an option to help consolidate the various inspections required in the field while still accomplishing all required tasks.

TWIC Implementation branch members worked directly with counterparts at TSA to discuss and address TWIC program improvements and issues. TSA has recently begun implementation of a civil enforcement program for individual TWIC holders violating regulatory requirements. Many Transportation Security Inspectors – Surface (TSI-S) personnel have reached out to Districts and Sectors to coordinate implementation of this inspection program and CG-FAC highly encourages units to support these efforts by TSA. CG-FAC has sent out specific guidance regarding this issue via CGMS. If units have specific questions or issues, please contact the TWIC Branch staff.



Rulemakings

Transportation Worker Identification Credential (TWIC)

The TWIC reader rule requires owners and operators of certain MTSA regulated vessels and facilities to use electronic readers designed to work with TWICs as an access control measure. The Coast Guard published the TWIC reader rule on August 23, 2016 with a two year implementation period.

Consolidated Cruise Ship Regulations

The Coast Guard will be adding requirements for screening baggage, personal items, and persons – including passengers, crew and visitors – intended for carriage on a cruise ship. New screening regulations will enhance the Coast Guard's broad role and responsibility for maritime security. The rule will strengthen cruise ship security, further enhancing the overall security of passengers. The Coast Guard is still developing this final rule.

Training

In 2016, Training Center (TRACEN) Yorktown graduated 47 students from the Waterfront Facilities Inspection course and 68 students from the Explosive Handling Supervisor course. TRACEN Yorktown also introduced the use of iPads as a training tool for students, replacing the use of printed course materials and hard copy CFRs and other references.

In early 2016, CG-FAC, in conjunction with TRACEN Yorktown and FORCECOM, initiated a Job Task Analysis (JTA) for the Waterfront Facilities Inspector course. Data collection for this JTA was collected through a survey administered electronically to field units, and it was in addition to a recently completed Container Inspection Training and Assistance Team (CITAT) course JTA. The emphasis of a JTA is ob performance. Job performance determines what will be evaluated, what should or should not be included in a training program, how much will be taught, and the instructional sequence. The end result of a JTA process is a final report that contains a list of tasks that have been rated by performers in the field, according to the Difficulty, Importance and Frequency (DIF) of each task.

The task list is then analyzed to produce recommendations for each of the tasks which are utilized by Program Managers, Training Managers, and TRACEN to determine which tasks should be selected for formal or on-the-job training, job aids (with or without training), and which tasks require no intervention at all.

TRACEN Yorktown and CITAT have been working on instructional systems design and development to redesign the CITAT course, and will pilot the new course in 2017. Starting in 2017, TRACEN Yorktown will lead efforts and provide support to CG-FAC in the redesign of the Waterfront Facilities Inspection course.

CITAT numbers

CITAT Container Inspection course graduates: 216, including 18 Department of Defense and Customs personnel (2 resident courses; 10 exportable courses)

CITAT trained 40 industry and Pipeline and Hazardous Materials Safety Administration personnel at the Transportation Safety Institute and assisted at two Multi-agency Strike Force Operations (MASFO's). For the year, CITAT assisted Coast Guard units with the inspection of 123 containers while providing high quality training.

CITAT supported the Department of Defense on four installation visits by training 62 additional personnel, assisting in the packing of 114 containers, and inspection of 209 containers, where they found 423 discrepancies. Without this assistance, vital DOD supplies could have been detained in ports around the world and negatively impacted DOD mission execution.

Area Maritime Security Committees

Area Maritime Security Committees (AMSCs) are a vital partnership to ensure the security of the maritime transportation system.

AMSC support

Using the Area Maritime Security Training and Exercise Program (AMSTEP), Federal Maritime Security Coordinators and their Area Maritime Security Committees (AMSCs) tested the effectiveness of their respective port-level AMS Plans and supported maritime security preparedness regimes through the engagement of federal, state, local, tribal, and territorial government and private sector stakeholders. In 2016, ninety-three (93) events were held, including 11 seminars, four workshops, 28 table top exercises, 11 functional exercises, 21 full-scale exercises, 12 area maritime security drills, one area maritime security game, and five maritime security operations during real events receiving exercise credit. Each event generated remedial actions for improving maritime security and identified best practices that were shared with the AMSCs.

AMSC of the Year

In April 2016, the Hawaii and American Samoa Area Maritime Security Committee was recognized as the AMSC of the Year. CG Sector Honolulu, the University of Hawaii (UH) and the AMSC jointly developed a cyber security exercise that consisted of a one and a half day operationally-based cyber exercise. During the exercise, information technology (IT) professionals utilized UH's *Cyber Range* to respond to attacks on the computer network systems associated with simulated container shipping and inter-island tug and barge companies. The cyber portion then became the basis for a half day discussion-based tabletop for senior-level port partners. Over 120 individual participants joined the exercise, representing 50 separate companies, government agencies, and maritime stakeholders from Hawaii, Guam, DC, California, Miami, and Houston.

Rear Admiral Richard E. Bennis Award for Excellence in Maritime Security

In 2016, CG-FAC was proud to identify the winners of the second bi-annual Rear Admiral Richard E. Bennis Awards for Excellence in Maritime Security. This award serves to highlight and recognize outstanding achievements and contributions of the maritime community with regards to implementation of Maritime Transportation Security Act (MTSA) requirements and other maritime security best practices in safeguarding our nation's Marine Transportation System (MTS).

The intent was to recognize organizations that demonstrate a true comprehensive culture of security. In addition, the award serves as a tool to encourage organizations to assess their overall security program to identify strengths and weaknesses, seek creative solutions for addressing known risks, build a system of continuous improvement, and share best practices that would benefit similar organizations.

The award selection committee collectively reviewed outstanding applications to identify the most distinguished submissions while recognizing the superior achievements and contributions of all in safeguarding our nations MTS. The 2016 recipients were:

A. Port Authority: Virginia Port Authority
B. Large Facility: Cheniere Sabine Pass Terminal
C. Small Facility: Port of Port Angeles
D. Large Company: Bridgeport and Port Jefferson Steamboat Company

This award honors Rear Admiral Richard E. Bennis, an exemplary Coast Guard leader who embodied Coast Guard core values and demonstrated an exceptional commitment to the security of the United States and the MTS. The late Rear Admiral Bennis began his career in 1972 as a graduate of the University of Rhode Island. He went on to serve as Captain of the Port Charleston, South Carolina, and Hampton Roads, Virginia. On September 11, 2001, while serving as Captain of the Port New York, Rear Admiral Bennis organized the extraordinary waterborne evacuation of nearly 500,000 people from lower Manhattan after the terrorist attacks on the World Trade Center. Rear Admiral Bennis served honorably in the Coast Guard for 30 years until his retirement in 2002.

Trending Issues in Port Safety, Security, and Resilience

Maritime Transportation System Recovery Unit (MTSRU)

CG-FAC collaborated with Areas and field units to discuss the expansion of the Marine Transportation System Recovery Plan (MTSRP) to address recovery from incidents other than maritime security related events. The Security and Accountability For Every Port Act of 2006 (or SAFE Port Act, Pub L 109-34) required the Area Maritime Security Plans to establish area response and recovery protocols to prepare for, respond to, mitigate against, and recover from a Transportation Security Incident. However, these protocols are just as applicable to other non-security related incidents, such as oil/hazardous material release, natural disaster response, mass rescue operations, and other contingencies. CG-FAC worked with CG Headquarters and Transportation Security Administration offices to determine the appropriate information safeguards of the MTSRP. CG-FAC also formed a workgroup comprised of Area, District and Sector representatives to enhance the MTSRP format and content for use during multiple incident responses. The updated plan template was shared with the Security Specialist (Port/Recovery) community during the 2017 National Advanced MTSRU Workshop.

CG-FAC participated in the 2016 Cascadia Rising exercise that trained, tested, and evaluated the whole community approach to complex disaster operations with city, county, state, federal, tribal, and military agencies and commercial businesses working together as a team. The exercise simulated a 9.0 magnitude earthquake along the Cascadia Subduction Zone (CSZ) and resulting tsunami along the Pacific Northwest. CG-FAC observed the response of Area and District personnel to identify gaps in policy related to regional MTS recovery. Lessons learned from natural disasters and contingency planning exercises identified the importance of MTS recovery policy to address regional coordination and communication following a transportation disruption. CG-FAC and Areas are updating policies to discuss coordination with Federal and state Department of Transportation (DoT) representatives and Federal Emergency Management Agency (FEMA) Emergency Support Function One (ESF-1) personnel managing transportation issues. Area representatives are scheduled to participate in U.S. DoT ESF-1 annual training to discuss the Coast Guard role in MTS recovery and coordination with other stakeholders.

The Customs and Border Protection (CBP)/Coast Guard Joint Protocols for the Expeditious Recovery of Trade were updated to reflect current CBP and Coast Guard Leadership as well as the Communications Flow Chart and Protocol Participation Matrix. CG-FAC continues to discuss MTS recovery planning and coordination with its CBP counterparts during national level exer-

cises and real world events, with the most recent engagement taking place in preparation and response to Hurricane Matthew. CBP is an important federal partner in MTS recovery and updating the protocols reflects this continued partnership.

Cyber risk management and impacts of a cyber incident to the MTS continues to be an area of great importance to the Coast Guard. The rapid evolution of cyber technology has a substantial impact on the MTS in term of efficiency and cyber risks. CG-FAC is in the process of incorporating MTS recovery elements in cyber policy for facilities and commercial vessels. The MTSRP and MTS recovery policy will be updated as cyber policies for facilities and vessels are promulgated.

What to Expect in 2017

- CG-FAC will continue working with the appropriate offices to develop cyber policy that will address training, exercises and cyber risk management for facilities and vessels.

- In 2017, CG-FAC-1 will work on initiatives related to MTS Recovery that include:

  -Updated MTSRP template;
  -Updated MTS Recovery Planning and Operations policy (COMDTINST 16000.28(series));
  -Updated Common Assessment Reporting Tool User's Guide

- CG-FAC-2 Safety Branch is working on numerous projects to update existing and create new policies. Keep an eye on the message board, FAC Notes, and your email for ways you can help shape these policies, and release of information when updates are completed.

- CG-FAC-2 will continue to evaluate ways to leverage iPads and other technology in use throughout the program to enhance mission execution while reducing the administrative workload burden on facility inspectors.

Office of Port and Facilities Compliance
Contact List

Office Chief

Captain Ryan Manning	202 372-1080

Domestic Ports (CG-FAC-1)

CDR Nick Wong (CDR Tim Grant; summer 2017)	202-372-1107
Mr. Ryan Owens	202-372-1108
Ms. Marilynn Small	202-372-1092

Port Resiliency/Recovery Branch

LCDR Christopher Pisares	202-372-1116
LCDR Rachel Stryker	202-372-1160
Mr. Rogers Henderson	202-372-1105
Mr. Chris Dougherty	202-372-1157
LT Niya Williams	202-372-1166

Critical Infrastructure (Cyber, & Port Security Specialists)

LCDR Josephine Long	202-372-1109
LCDR Brandon Link (summer 2017)	
Mr. Jason Warren	202-372-1106
Mr. Robert Reimann	202-372-1146
Dr. Robyn Kapperman	202-372-1110
LT Damon Sanders	202-372-2151

Cargo and Facilities (CG-FAC-2)

CDR Frances Fazio	202-372-1171
Mr. Jim Bull	202-372-1144

Facility Safety (explosive handling, containers, COAs)

LCDR Daniel McQuate	202-372-1130
LT Laura Gould	202-372-1114
MSTC Gregory Becker	202-372-1127
Captain David Condino	202-372-1145

Facility Security (MTSA)

LCDR Adam Cooley	202-372-1132
Mr. Casey Johnson	202-372-1134
Ms. Betty McMenemy	202-372-1122

TWIC Implementation

LCDR Brett Thompson	202-372-1154
LT Bill Gasperetti	202-372-1139

Security Standards (Regulation Development)

LCDR Kevin McDonald	202-372-1168
LCDR Yamaris Barril (Summer 2017)	
LT Angela Alonso	202-372-1151

USCG TWIC Help Desk	202-372-1139 TWIC.HQ@uscg.mil

CG-FAC Links

www:	http://www.uscg.mil/hq/cg5/cg544/default.asp
Portal:	https://cgportal2.uscg.mil/units/cgfac/Documents/Forms/AllItems.aspx
Homeport:	Homeport> Mission> Maritime Security or Ports and Waterways
TWIC (Portal):	https://cgportal2.uscg.mil/communities/twic-discussion/SitePages/Home.aspx