



DEPARTMENT OF HOMELAND SECURITY

UNITED STATES COAST GUARD



OFFICE OF PORT AND FACILITY COMPLIANCE

2015 ANNUAL REPORT

Table of Contents

Executive Summary	1
Highlights of 2015	2
Cyber Security	8
2015 Port Facility & Cargo Security Compliance Performance	12
Container Updates	13
2015 TWIC Verifications	15
2015 MTSA Facility Enforcement Actions	16
Rulemakings	18
Training	19
Area Maritime Security Committees	21
Trending Issues in Port Safety, Security, and Resilience	22
What to Expect in 2015	25

CG-FAC Policy Review

Throughout this document various policy, instructional, 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

Hanjin Shipping Terminal, Port of Long Beach California.

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.

As this document demonstrates, CG-FAC remains on the forefront of developing guidance to address a myriad of new technologies and risks in the maritime community, from Unmanned Aerial Systems to the use of Liquefied Natural Gas as fuel, to cyber risk management, which continues to dominate the conversation of new threats to maritime infrastructure. Both the public and private sectors are increasingly dependent on cyber systems for routine and emergency services, and like other systems they are vulnerable to accidents, natural disasters, and deliberate attacks. CG-FAC began working with the field and industry partners in many settings and has issued several policy documents and resource lists to help stakeholders begin to address their cyber vulnerabilities. In January of 2015, we held a public meeting to further this process.

In other major developments, 2015 saw the signing of the "Strategy for the Waterside Security of Especially Hazardous Cargo". The development of this Strategy was a multi-year effort bringing together public and private stakeholders to address a myriad of complex issues associated with the movement of hazardous cargo. Ultimately, this strategy will manage the risk of an attack on the Maritime Transportation System (MTS) involving EHC by mitigating the Threat, Vulnerability, and Consequence elements of risk through the Awareness, Prevention, Protection, Response, and Recovery components of the security spectrum.

Most of all, CG-FAC is extremely proud to support the Coast Guard men and women who in 2015 completed over 12 thousand facility inspections (20% of which were MTSA compliance inspections), over 48 thousand visual and electronic inspections of TWIC cards, and more than 24 thousand container inspections. Maintaining that strong operational presence on the waterfront is key to safe, secure ports. 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 Andrew E. Tucci, USCG

Highlights of 2015

National Strategy for the Waterside Security of Especially Hazardous Cargo (EHC Strategy)

On 1 September 2015, the Commandant of the Coast Guard signed the "Strategy for the Waterside Security of Especially Hazardous Cargo." As mandated by DCO Functional Statements, CG-FAC is responsible for the policy for the maritime transportation of EHC including Liquefied Natural Gas. CG-FAC oversaw the drafting



and addressing of comments and questions from DHS, OMB and the NSC. The EHC Strategy reflects the input and collaboration of Federal, state, and local government agency, maritime industry, and private sector stakeholders. It seeks to manage the risk of an attack on the Maritime Transportation System (MTS) involving EHC by mitigating the Threat, Vulnerability, and Consequence elements of risk through the Awareness, Prevention, Protection, Response, and Recovery components of the security spectrum. Security governance to facilitate and improve communication between industry and government on incident response/recovery, as well as maritime transportation infrastructure security, will be incorporated through an Implementation Plan. CG-FAC is working an initial action plan with a 5 year execution.

A special thanks to James Prazak at Tricon Energy Ltd. for his help at every stage (i.e., cargo security symposium, workgroups, public listening sessions, etc.) of the EHC National Strategy, Geoff Powers, Mark Willis, Eric Golder and Dave Stalford of ABS Consulting who were mainly facilitators of workgroups and listen sessions which were all vital to the promulgation of the EHC National Strategy, Jennifer Carpenter and Brian Vahey at American Waterways Operators for reaching out to the tugboat, towboat and barge industry for a myriad of EHC issues, and James Battese at Miami Nation in Oklahoma for his help with all the national, state, local, tribal and territorial EHC issues

Highlights of 2015

Technology



CG-FAC-2 completed initial distribution of iPads to Facility Inspection teams at units that requested to be part of the program in 2014. This will reduce the need to carry large quantities of references and materials that could weigh near 30 – 40 pounds. Facility Inspectors have provided some great feedback on how they are using the iPads as well some great suggestions for future application. Other Sectors that were not on the initial distribution have heard of the recent success and implementation of the iPads in the field and requested to be part of the program. CG-FAC purchased 120 more

devices, sent them to the remaining units, and paid for another year of the Mobility Standard recurring cost. Other devices which FAC recommends purchasing, at the unit's expense, are a Bluetooth keyboard, portable Bluetooth printer, and Apps. Recommended Apps to purchase are PDF Expert, Word, Excel, Weather (any), and Notes Plus. We would appreciate any feedback and recommendation for use of the iPads provided to the CG-Portal site. <https://cg.portal.uscg.mil/units/cgfac2/iPads/SitePages/Home.aspx>

PSS Program

Front End Analysis: In September 2015, the Performance Technology Center conducted a new performance planning front end analysis (FEA) to determine Port Security Specialist and Security Specialist (Port / Recovery) performance requirements. The FEA began in December 2014 with a thorough review of existing directives pertaining to the PSS and SS (P/R) performance. The analysis team collected data from subject matter experts and accomplished performers to recommend performance support interventions. Ten recommendations were identified during the FEA. Recommendations from this analysis will help optimize limited training resources and improve Port Security Specialist and Security Specialist (Port / Recovery) performance. CG-FAC with working with FORCECOM to develop a Performance Support System for both the Port Security Specialist and Security Specialist (Port / Recovery).

PSS ALCOAST: In August 2015, CG-FAC released an ALCOAST providing an update to the PSS Program. The ALCOAST defined roles and responsibilities of the PSS, and

Highlights of 2015

highlighted accomplishments of the PSS Community.

A Special Thanks to Jon Hatt and LCDR Julie Kuck at PTC Yorktown for heading up New Performance Planning (NPP), Front End Analysis (FEA) for the Port Security Specialist (PSS) and Port Security Specialist Recovery (PSSR) job series, PSS Accomplished Performers (AP) Jim Armstrong, John Bray, Rick Sorrell and John Walker for their help with PSS workforce task list refining and task measurement SS (P/R), and Doug Campbell, Kevin Blount and Tim Lupher for their help with SS (P/R) workforce task list refining and task measurement

Cybersecurity Assessment and Risk Management Approach (CARMA) Assessment in Philadelphia

CG-FAC continues to look for tools that can assist ports in identifying cyber vulnerabilities within their ports. During the week of June 8th, a host of federal agencies, along with industry port stakeholders came together at Sector Delaware Bay in Philadelphia, Pennsylvania to tackle cyber risk management. DHS Office of Sector Engagement Critical Infrastructure Resilience, in conjunction with the Coast Guard, led a cyber risk assessment in the Port of Philadelphia. This was a great example of federal agencies coming together to try and assess cyber risks within a port. Along with DHS, other federal agencies present included National Institute of Standards and Technology (NIST), Federal Energy Regulatory Commission (FERC), Customs and Border Protection (CBP), Transportation Security Administration (TSA). From the Coast Guard, members from Sector Del Bay, LANTAREA, CG-FAC, CG-CVC were also represented.



Marine Pollution Prevention, MARPOL, ISO, PAME

CG-FAC staff served as expert representatives on several international organizations and covering a wide range of issues critical to the nation's environmental, and maritime safety and security strategies.

First, staff members served on the Arctic Council's Protection of the Arctic Marine Environment (PAME) working group, and, as chair of PAME's Regional Reception Facility Expert Group, attended two international meetings and authored or contributed to numerous international papers reporting on development of regional arrangements for port reception

Highlights of 2015



facilities, shipping in the Arctic, marine debris in the Arctic, and information on current state of shipping and port infrastructure in the Arctic.

CG-FAC staff attended and delivered a paper and presentation on waste from ships and pollution in the Arctic to the World Maritime University/IMO ShipARC 2015, international conference on shipping in the Arctic. For more information and view all the presentations visit

the conference website at: <http://commons.wmu.se/shiparc/>

CG-FAC staff also served as CG representative for Interagency Marine Debris Coordinating Committee (IMDCC) and initiated work on USCG Section of the IMDCC biennial 2014-2015 Report to Congress. The report will be finalized later this year and will detail CG efforts to mitigate marine debris in the marine environment.

Additionally, CG-FAC staff provided representation at the American National Standards Institute at the annual plenary session of the International Organization for Standardization (ISO) Technical Committee 8, Subcommittee on Marine Environmental Protection (ISO/TC8/SC2). We served as chair of Work Group 4 on shipboard waste management and reviewed two existing standards for managing MARPOL wastes and Port Reception Facilities for updates and publication of 2nd editions (expected 2016).



As part of CG-FAC outreach efforts, staff participated in and addressed three national events sponsored by the North American Marine Environmental Protection Association on MARPOL and USCG port reception facility program issues.

In conjunction with completing a review and updates for a NVIC addressing reporting of inadequacy at MARPOL port reception facilities, CG-FAC-2 also updated and received OMB approval for Certificate of Adequacy application forms CG-5401 A, B, and C. Additionally a new form CG-5401 D received OMB approval and will be available as soon as associated MARPOL Annex VI regulation are published. The updated forms are

Highlights of 2015

available at the USCG Electronic Forms website at: <http://cgweb.comdt.uscg.mil/CGForms/Welcome.htm>

Coast Guard LNG Workgroup

CG-FAC continues to chair the LNG Workgroup, and during this last year the work group facilitated the development and release of OES Policy letters 01-15 and 02-15 to, among other things, address gaps in 33 CFR 127 for LNG facilities that will bunker LNG. As the industry continues to grow in this area, the LNG workgroup brings representatives across the Coast Guard to discuss the issues and advise leadership. Both Harvey-Gulf and TOTE have delivered vessels with LNG fueled engines, and the LNG workgroup worked closely with field units to interpret regulations and develop implementation strategies for these new facilities. Units that are interested in participating in the LNG Workgroup are welcome to contact CG-FAC Facility Safety Branch, or check out the LNG Workgroup site in CG Portal. <https://cg.portal.uscg.mil/units/cgfac2/LNG%20%20CNG/Forms/AllItems.aspx?RootFolder=/units/cgfac2/LNG%20%20CNG/Natural%20Gas%20Facility%20Workgroup/Workgroup%20Meetings>



LNG Bunkering in Jacksonville : This is part of the first bunkering operations in Jacksonville, FL, while conducting container loading operations. The vessel is the M/V ISLA BELLA the first ever purpose built LNG Container ship. This picture captures bunkering operations transferring LNG from truck to vessel.

Highlights of 2015

Alternative Security Program

The Alternative Security Program (ASP) continues to benefit the public, the Coast Guard, and the maritime industry by providing a flexible approach to managing security risks. There are close to 200 facilities operating under ASPs and thousands of vessels, more than are using vessel-specific security plans. CG-FAC is pleased to work closely with industry groups to keep our ports and waterways safe and secure.

During the past year, two ASP Sponsoring Organization's Workshops were held in Washington, DC. These workshops are a great forum for information sharing and discussions of best practices for both facilities and vessels. The workshop, held on November 18, 2015, provided an opportunity for in-depth discussions on cyber risks. Since cyber-security is a topic of growing interest to the entire maritime industry the Coast Guard is exploring options for how to best incorporate cyber risks into security plans required by the Maritime Transportation Security Act. Many industry groups are developing cyber security best practices and the Alternative Security Program potentially provides an ideal way of addressing cyber risks. We appreciate the cooperation of all ASP plan holders in helping the Coast Guard identify and address cyber risks. A special thanks to Bill Erny of the American Chemistry Council for his leadership in addressing cyber security risks for ACC facilities.

Alternative Security Program Members

American Chemistry Council	American Gaming Association
American Waterways Operators	Liquid Bulk Terminal Alternative Security Program
Greater NOLA Barge Fleeting Association	Lake Carriers' Association
North American Export Grain Association	National Grain & Feed Association
Offshore Marine Service Association	Passenger Vessel Association
Washington State Ferries	

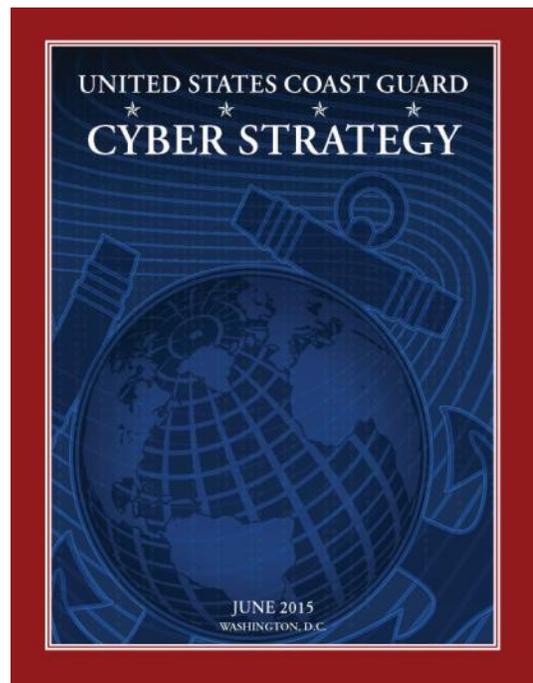
Cyber Risk Management



On 15 January 2015, CG-FAC held a public meeting to solicit input on a policy development project to address cyber security risks in the marine transportation system. The meeting took place at the Department of Transportation building in Washington DC. Presenters included VADM Michel, RADM Lytle, RDML Thomas, along with representatives from NIST, NRC, and ICS CERT. Attendees included representatives from across the maritime industry, including vessel and facility operators, major industry associations, academia, and others. Reporters from Politico and InsideCybersecurity.com were also present. Anticipating strong interest, CG-FAC worked with CG-092 and DOT to establish live video/YouTube capability, a first for a Coast Guard public meeting. This effort proved successful, as over 100 streams watched the meeting live, with over 200 more viewings w/in 24 hours (<https://www.youtube.com/embed/rzOVc1ZOuvY?rel=0>).

In June 2015, the Commandant announced the promulgation of the Coast Guard's first Cyber Strategy. This Strategy presents a ten-year vision for Coast Guard operations in cyberspace, and lays out our Service's highest strategic objectives in this rapidly evolving operational domain. As the Commandant indicated, cyber technology poses opportunities and challenges for the Coast Guard across all our missions, and is inextricably linked with our ability to ensure the Safety, Security, and Stewardship of our Nations waters in the 21st Century. The Coast Guards Cyber Strategy includes three priorities that

directly support the integrity of our own systems and networks, enable our diverse operations, and help protect our nation's maritime critical infrastructure and the MTS. CG-FAC played and continues to play a major role in the Protecting Infrastructure priority identified within the Strategy (<http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>).



Cyber Risk Management

With the signing of the Cyber Strategy, CG-FAC became the lead office for implementing the Protect Infrastructure portion of the Strategy. The newly formed Protect Infrastructure Cyber Strategy Implementation Team (CSIT) had representatives from nearly every office within CG-5P and also representatives from other offices including CG-2, CG-6, and CG-5R. Other offices outside of HQ have also pitched in, including National Maritime Center (NMC), Areas and Districts, just to name a few. The CSIT recently submitted an implementation plan and continues to work to complete identified initiatives.

Cyber Lexicon

CG-FAC, working within the Transportation System Sector Cyber Security Working Group, assisted in developing a Common Cyber Language for the Transportation Sector. The language is a testament to the dedicated Public/Private partnership that is fostered in the Transportation Sector, and can be used to assist sub-sectors such as airlines or rail within the Transportation Sector have a common language when discussing cyber issues. The Common Cyber Language can be found on Homeport under the Cybersecurity Missions Tab in Cyber Info.



Cybersecurity Assessment and Risk Management Approach (CARMA)

CARMA is a DHS developed tool that attempts to identify cyber risks within the port. It is a stakeholder-vetted list of the Port's cyber infrastructure, as defined by its critical functions, supporting value chains, and specific types of cyber systems. What is important is that it utilizes local stakeholders to derive a port-level understanding of shared vulnerabilities and with it a prioritized list of strategies for managing the identified risks. This allows individual owners and operators to prioritize budget and resource allocations according to common risks. It also uses the identified cybersecurity risks to help build valid scenarios that could be leveraged for sector- or national-level cyber exercises.

Cybersecurity Resiliency Review (CRR)

CRR is a review of the overall practice, integration, and health of an organization's cybersecurity program. The CRR seeks to understand cyber security management of services (and associate assets) critical for an organization's mission success by focusing on protection and sustainment practices within key areas that typically contribute to the overall cyber resilience of an organization.

Cyber Risk and Research

CG-FAC members were active in supporting Coast Guard wide research and development related to cyber risks in the marine transportation system.

In March, CG-FAC co-sponsored the first ever maritime cyber research workshop at the DHS Center of Excellence at Rutgers University. Working with Dr. Fred Roberts at the Command, Control, and Interoperability Center for Advanced Data Analysis, Coast Guard and other partners discussed cyber challenges ranging from GPS vulnerabilities to industrial control systems on waterfront facilities. Vice Admiral Michel, then the Deputy Commandant for Operations, attended and identified a number of cyber questions for further research.



Only a few weeks later, CAPT Tucci delivered opening remarks at a Coast Guard Academy hosted workshop that addressed MTS and other cyber challenges for the Coast Guard. Coast Guard Academy Cadets are studying cyber risks in the Marine Transportation System, and are helping CG-FAC identify training programs suitable for Coast Guard facility and vessel inspectors.

The research begun at Rutgers University and CCICADA continued in June at the California Maritime Academy. With 76 attendees across every level of government, plus academia and the private sector, the event drew on a talented and diverse group. Among other luminaries, Captain Bruce Clark of CAL Maritime, Dr. Nicole Drumhiller of American Military University, and Dr. Roberts of CCICADA lent their considerable talents to making this event a success. Dr. Joe DiRenzo of the U.S. Coast Guard's Research and Development Center is working with CG-FAC to plan and coordinate further cyber research efforts.



CG-FAC personnel collaborated with other groups grappling with the challenges of cyber risks in the maritime domain, including the Transportation Research Board of the National Academies and the Bureau of Safety and Environmental Enforcement. This work is helping to build the Coast Guard's cyber expertise, gain understanding of how the cyber and maritime domains interact, and leveraging the lessons learned and best practices from other organizations.



Cyber Risk Awareness and Policy Development

The work with the RDC and others in Academia was one component of several efforts designed to improve the Coast Guard's knowledge of cyber risks in order to develop effective policy.

In 2015, the Coast Guard worked with the National Maritime Security Advisory Council, the National Offshore Safety Advisory Council, and many individual industry associations to share cyber information.

In June, the U.S. Coast Guard submitted a paper and introduced cyber risk management as a topic at the International Maritime Organization. Transport Canada has been a particularly strong partner in cyber, and we are working to develop similar policies which will reflect the international nature of cyber risk and minimize burdens on industry doing business in both countries.

CG-FAC sent out 12 cyber related notices in 2015. A new resource section was also added to Homeport that shares over 100 different links to cyber related sites from advisories to alerts, assessment tools, recovery resources, supporting documents, tools, and training and education (Found under the "Links to other Cyber related sites" section of the Cybersecurity Missions Tab).

A SPECIAL THANKS TO:

Matt Barrett and Don Tobin at National Institute of Standards and Technology (NIST) for their support of COMDT's Cyber Strategy in creating an NIST Cybersecurity Framework Implementation Guide.

Peter Sindt at TSA for managing the Transportation Specific Sector Cybersecurity Working Group.

April Danos with AAPA for her ongoing support of the COMDT's Cyber Strategy.

Aaron Padilla at API for supporting the Bulk Liquid Transfer NIST Cyber Framework Implementation Guide.

Dan Strachan at AFPM for supporting the Bulk Liquid Transfer NIST Cyber Framework Implementation Guide.

Kelly McClelland and Patrice Delatte, co-leads of the NOSAC Cybersecurity Sub-Committee, for their continued work in Cyber Risk Management in the offshore industry.

2015 Facility Inspections Program Statistics

Total regulated facilities:	8,211
<i>MTSA-regulated facilities:</i>	<i>3,476</i>
Total facility inspections completed:	11,856
<i>MTSA facility inspections completed:</i>	<i>5,937</i>
Total container inspections completed:	18,053
Total transfer monitors conducted:	456
Total operational controls (COTP Orders)	34
<i>Security COTP Orders</i>	<i>16</i>
<i>Safety/Environmental Protection COTP Orders</i>	<i>19</i>

2015 MTSA Security Compliance by District

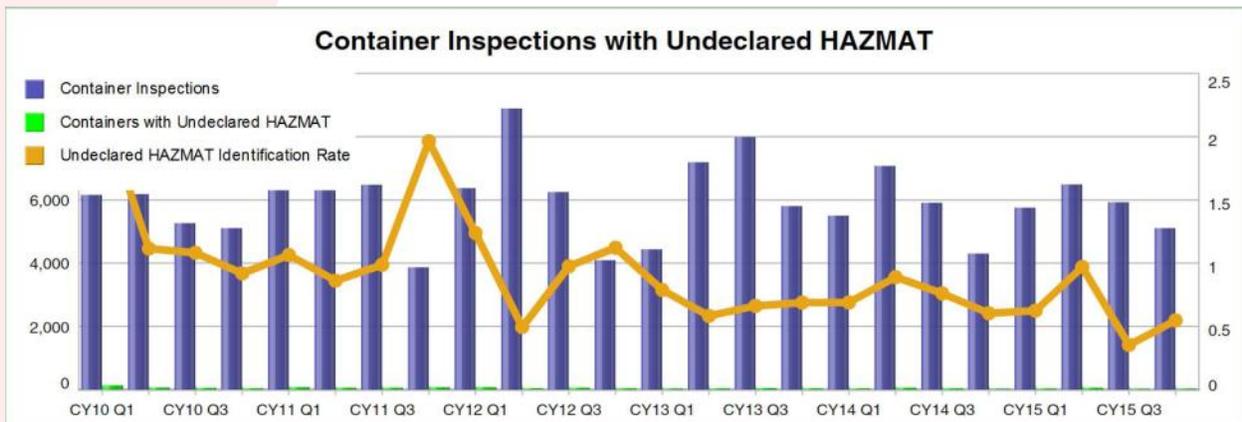
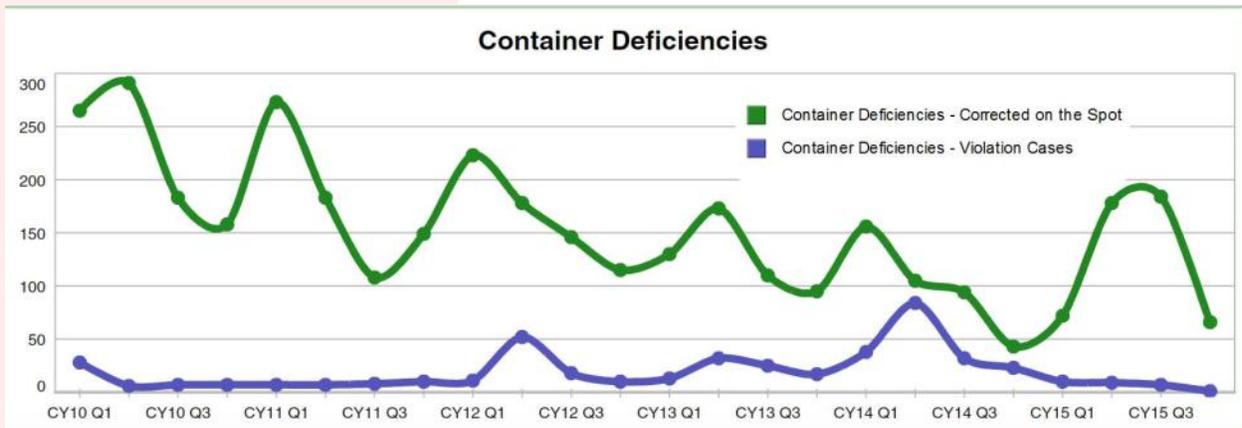
District	FSPs*	MTSA Inspections	Deficiencies
1st	298	949	164
5th	166	451	129
7th	310	928	241
8th	905	1902	570
9th	304	691	120
11th	135	326	120
13th	139	257	106
14th	77	214	142
17th	98	219	27
Total	2432	5937	1619

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

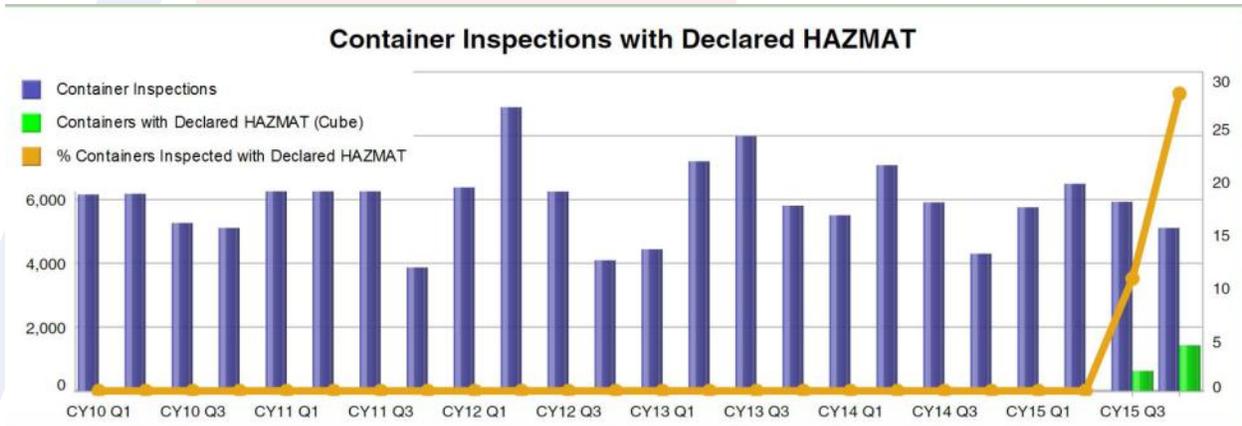
Container Updates

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 ailing the shipment of containers and account for 86% of deficiencies according to 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 inspecting containers with declared hazardous materials and includes such things as verifying paperwork and packaging requirements are met. General inspections contribute to identifying shipments of un-declared HAZMAT or other deficiencies with a container. Structural inspections occur during every container inspection 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.

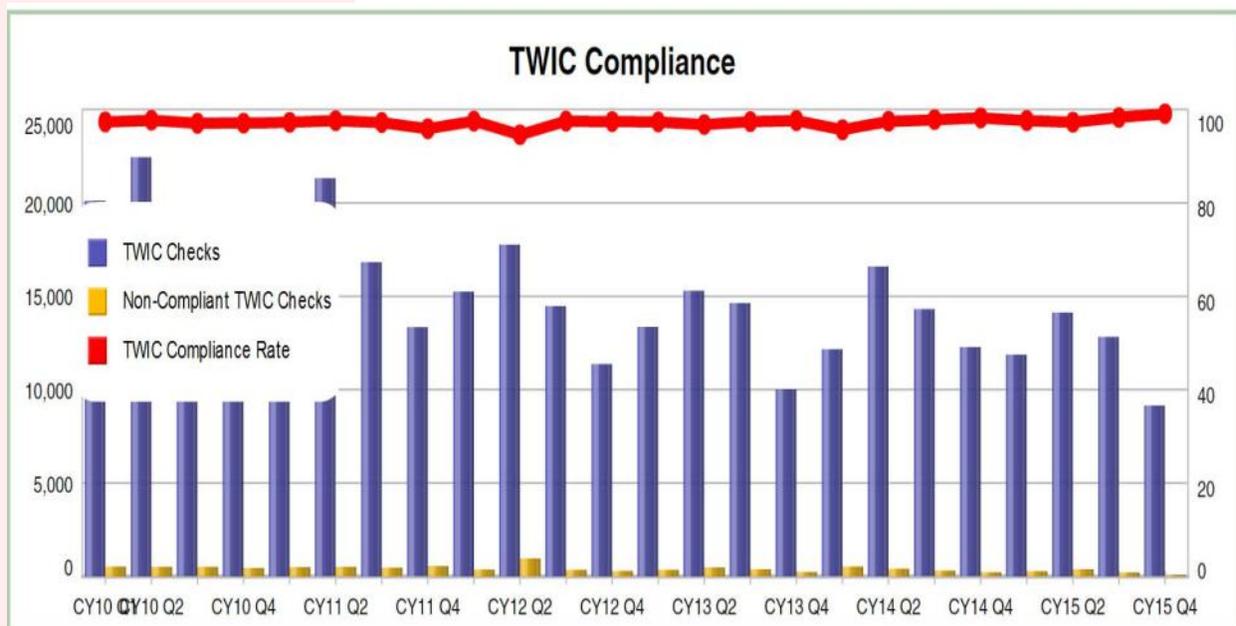
The new 50/50 model is an interim change to better identify all potential or existing risks in all types of containerized cargo shipments. CG-FAC will continue to monitor inspection results and data update the program and the field as needed. Input from the field is always welcomed and appreciated as 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 48,289 visual and electronic inspections of TWIC cards in 2015, and identified 970 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 publication 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 what is required in the field by inspectors 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.



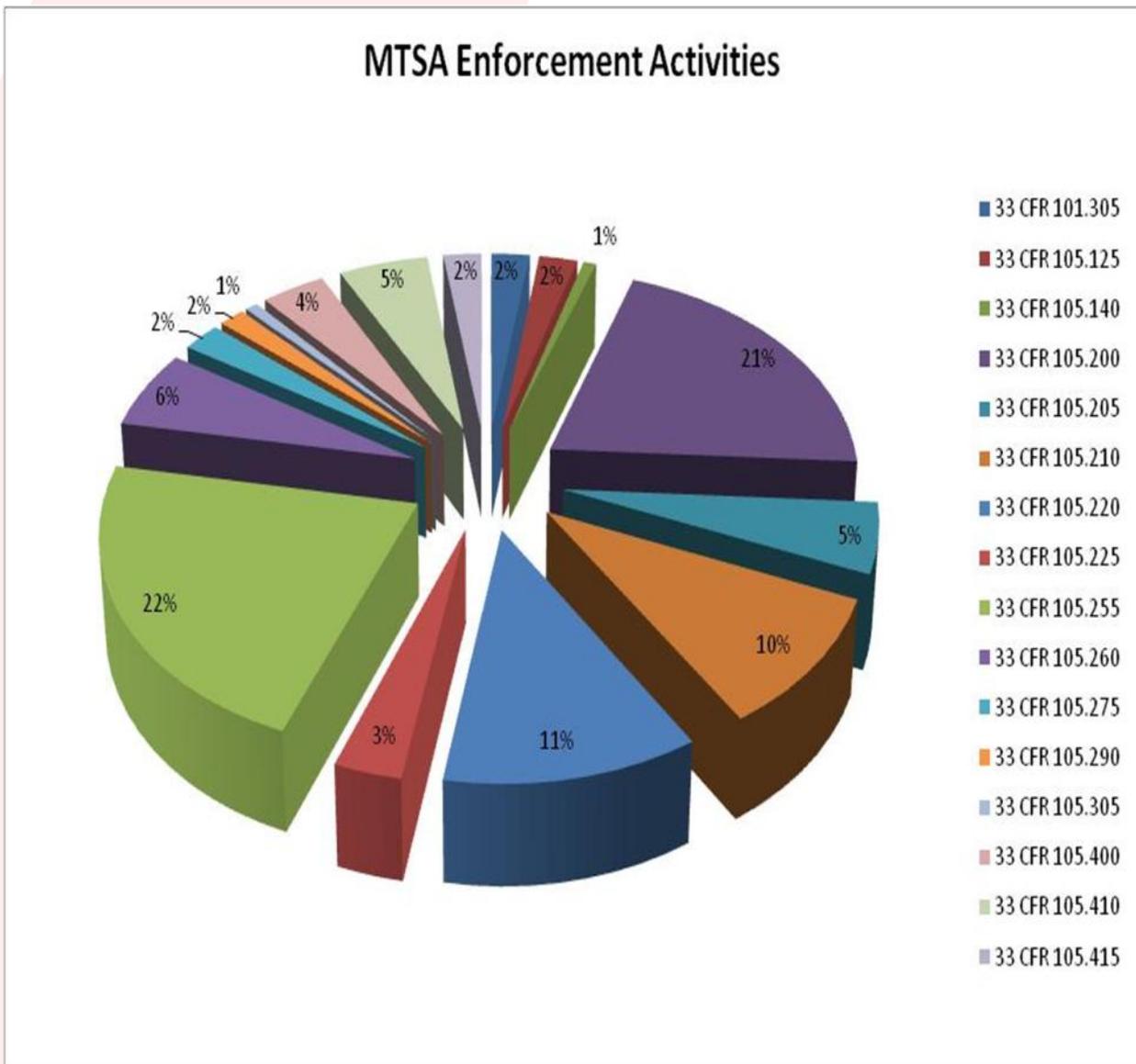
2015 MTSA Facility Enforcement Actions

In 2015, the Coast Guard completed 4,717 security-related MTSA annual and spot check examinations and recorded 131 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 131 enforcement activities executed in 2015 took place at 115 MTSA-regulated facilities and included official letters of warning or administrative civil penalties.

Citation	Citation Title	Enforcement Activities Executed
33 CFR 101.305	Reporting, Breach of Security	3
33 CFR 105.125	Noncompliance	3
33 CFR 105.140	Alternative Security Program	1
33 CFR 105.200	Owner or operator requirements	27
33 CFR 105.205	Facility Security Officer requirements	7
33 CFR 105.210	Facility personnel with security duties	13
33 CFR 105.220	Drill and exercise requirements	15
33 CFR 105.225	Facility recordkeeping requirements	4
33 CFR 105.255	Security measures for access control	29
33 CFR 105.260	Security measures for restricted areas	8
33 CFR 105.275	Security measures for monitoring	3
33 CFR 105.290	Additional cruise ship terminal requirements	2
33 CFR 105.305	Requirements for facility security assessments	1
33 CFR 105.400	Facility Security Plans	5
33 CFR 105.410	Facility Security Plans – Submission and approval	7
33 CFR 105.415	Facility Security Plans – Amendment and audit	3
Total		131

2015 MTSA Facility Enforcement Actions

As noted on the previous page, as in 2014, almost 50% of Coast Guard enforcement actions at regulated facilities were for 33CFR105.200 and 105.255 violations. As the new rulemakings develop into regulatory requirements, it will be increasingly important that facility inspectors work with Area Maritime Security Committees and individual facilities to ensure they are ready to meet all forthcoming regulatory mandates. At the same time, Captains of the Port are reminded that facility regulations are intended to be functional requirements. If facilities can meet the intended function of the regulation through an equivalency, we encourage Captains of the Port to work with the facilities and CG-FAC through the equivalency request and approval process.



Rulemakings

Seafarer’s Access to Maritime Facilities

On July 27, 2015, the public comment period for the Seafarer’s Access to Maritime Facilities Notice of Proposed Rulemaking (NPRM) officially closed. The 162 comments have been adjudicated and the Final Rule is being developed. This proposed rule would implement section 811 of the Coast Guard Authorization Act of 2010, and requires each owner or operator of a facility regulated by the Coast Guard to implement a system that provides seafarers and other individuals with access between vessels moored at the facility and the facility gate, in a timely manner and at no cost to the seafarer or other individual.

Consolidated Cruise Ship Security

On June 1, 2015, the public comment period for the Consolidated Cruise Ship Security Notice of Proposed Rulemaking (NPRM) officially closed. The 115 comments have been adjudicated and the Final Rule is being developed. The Coast Guard proposes to amend its regulations on cruise ship terminal security and the proposed regulations would provide detailed, flexible requirements for the screening of all baggage, personal items, and persons—including passengers, crew, and visitors—intended for carriage on a cruise ship. The proposed regulations would standardize security of cruise ship terminals and eliminate redundancies in the regulations that govern the security of cruise ship terminals.



Port of Miami Cruise Ship Terminal

Training

This year, CG-FAC traveled to each District to meet with a number of Facility Inspectors and Port Security Specialists during the FAC road show. Program staff covered certain topics specific to the Unit, District, or Area's request. Hot topics were LNG as Fuel, TWIC, MTSAIL, and Cyber. As always, if the field needs any assistance from Program on policies or procedures please send up a request through the Chain of Command, District, and Area and we will be happy to assist as needed.

Future Training Opportunity

Incorporated into the new Explosive Handling Supervisor Instruction (coming to a Unit near you) is the use of Quantitative Risk Analysis (QRA). A QRA is a further analysis of the highest priority risks during which a numerical or quantitative rating are assigned in order to develop a probabilistic analysis of the project. Tools that assist with calculating QRA are SAFER (used by DOD) and IMESAFER (used by Industry). Program has provided funding for an EHS Instructor and a Unit member to attend the Institute of Makers of Explosives (IME) training so it can be incorporated into the EHS course.

Schoolhouse Training

Facilities Inspections Workforce Training for Qualification and Proficiency

CG-FAC continues to remain actively engaged with the Port Operations School at TRACEN Yorktown, the Container Inspections Training and Assist Team (CITAT), as well as the training program within FORCECOM to enhance and improve the Waterfront Facilities course, the Explosive Handling Supervision course, and the Container Inspections course. This year a Job Task Analysis (JTA) is being completed for the Container Inspection course and one will be started for the Waterfront Facilities Inspections course. This will allow us to better align the training in the course with the job that is being done in the field. In addition to Coast Guard resident and exportable training, the National Cargo Bureau (NCB) offers exceptional training, specifically tailored for Coast Guard marine and facility inspectors and prevention personnel. CG-FAC highly encourages Sectors and field units to develop close working relationships with the NCB surveyors in their COTP zones. NCB provides a wealth of experience and expertise in not only container inspections and hazardous materials, but also marine inspections and general regulatory compliance.

Training

TRACEN Yorktown Waterfront Facilities Course graduates: 39

TRACEN Yorktown Explosive Handling Supervision Course graduates: 66

CITAT

CITAT Container Inspections Course graduates: 195 (2 resident courses; 9 exportable)

CITAT Container Inspections Course graduates: 195 (2 resident courses; 9 exportable)

In addition, CITAT trained 135 industry students at Transportation Safety Institute (DOT); 5 IMDG/Hazmat presentations; avg 15 students each and PHMSA (1 conference-2 presentations to 30 people each)

CITAT assisted units with 945 container inspections, of which 863 were done during 3 MASFOs (Sector Hampton Roads-2x; Sector New Orleans).

One DOD course provided: 18 U.S. Army Unit Movement Officers (UMOs). Overall in FY15 for DOD, they inspected 66 containers, identified 278 discrepancies, sealed 44 containers and trained 221 Army personnel.

Area Maritime Security Committees

Area Maritime Security Committees are a vital partner in securing the maritime transportation system.

AMSC support

\$253,617 in AMSC support funds were distributed throughout the AMSC's to enhance security measures, fund travel and training.



AMSC of the Year



In April 2015, the Delaware Bay Area Maritime Security Committee was recognized as the 2014 Area Maritime Security Committee of the Year. The Delaware Bay AMSC hosted and participated in a nine-day full-scale exercise called FRONTIER SENTINEL 2014. The exercise scenario involved the mining of the federal channel and anchorage in the Delaware Bay constituting a significant threat and impact to the Marine Transportation System supporting the key strategic ports of Philadelphia, Camden, and Wilmington, Delaware. The AMSC was also on the cutting edge by developing a Business Continuity Planning Project. This project consisted of a Regional Risk Assessment that analyzed the risks, hazards, and vulnerabilities common to maritime facilities. It also included a Regional Business Continuity Planning Template which was developed by taking an all hazards approach to include commercial risks, and applying guidelines that had been developed as part of the port-wide Strategic Risk Management Plan. The template document serves as a readily implementable tool for use by Port Stakeholders in developing their own Business Continuity Plans. Widespread use of this template will lead to facilities better suited to maintain critical business functions throughout our port and the nation, leading to a more secure, resilient port and the ability to continue to contribute to the regional economy through unforeseen circumstances.

Trending Issues in Port Safety, Security, and Resilience

Maritime Transportation System Recovery Unit (MTSRU)

CG-FAC has engaged with field units through developed policies, guidance and training focused on the importance of the MTSRU work. This will ensure stabilization and recovery of the Marine Transportation System (MTS) and resumption of commerce following a transportation disruption, which are vital to the lives of the citizens in the affected area (and beyond) and to the overall economic security of our nation. In order to build system continuity and maintain effective levels of program readiness, CG-FAC Senior Leadership developed and incorporated a strategy with the office business plan to host a National MTSRU Workshop every two years, to review and update program policies, guidance and analyze lessons learned from real events to improve response effectiveness and enhance program visibility.

CG-FAC hosted our first National Advanced MTSRU Workshop convening the Coast Guard civilian Port Security Specialist (Recovery) (PSSR) working group at Sector Los Angeles/ Long Beach from 31 MAR – 02 APR 2015 to review MTSRU program policies and practices. The PSSR working group was involved with mission review, training, planning and preparation of sound recommendations to improve the overall program guidance for response and recovery operations in order to minimize the consequences of national disasters, accidents and attacks that may threaten our ports.

2015 NATIONAL ADVANCED MTSRU WORKSHOP



"Supporting Port Resiliency and Improving Recovery Readiness Through Effective Planning, Preparation and Strong Partnerships"



Some of the Program and Policy recommendations following the National Advanced MTSRU Workshop were:

- Revisit verbiage in Policy Letter 13-01, "Policy For Use of The Common Assessment and Reporting Tool (CART)", dated 03 APR 2013, Section 5, as it relates to System Use requirements during transportation disruption affecting the MTS;
- Upgrade GIS technology and system capabilities in CART database to support MTS recovery;
- Coordinate with CG-CPE to prioritize MTSL Front-end Analysis (FEA) implantation by FORCECOM;

Trending Issues in Port Safety, Security, and Resilience

Maritime Transportation System Recovery Unit (MTSRU) (cont)

- Remove the MTS Recovery Plan from the Area Maritime Security Plan (AMSP) and develop an all hazards standardized stand-alone MTSR Plan;
- Develop policy and guidance for coordinating regional recovery efforts and qualifications beyond Type 3 MTSL incidents;
- Develop policy and guidance on a MTS Recovery Exercise Strategy that support all hazards incidents;
- Create an MTS Recovery Case Study Community in CG Portal or another outlet for awareness, recommendations, and field development;
- Re-emphasize to the field users the importance of maintaining CART Data Integrity Standards through validation and updates of Essential Elements of Information (EEI) required in CART Policy Letter 13-01; and
- Purchase and distribution to field PSSRs 50 stand-alone laptop computers and biometric hard drives to be used remotely during response and recovery operations to significant port disruptions.

CG-FAC has completed 60% of the above recommendations and will continue to work towards 100% completion in CY2016.

Cooperation with Transport Canada

Transport Canada has been a particularly strong partner with the U.S. Coast Guard. Mr. Scott Naugler of Transport Canada attended our MTSRU Workshop, and has led TC efforts on the Beyond the Border initiative on the Great Lakes, and in New England/Canadian Maritime. Working through the Maritime Security Working Group, Scott Naugler, Nora Johnson, and many others have helped the Coast Guard and Transport Canada to improve our mutual security. We look forward to increased cooperation in 2016.



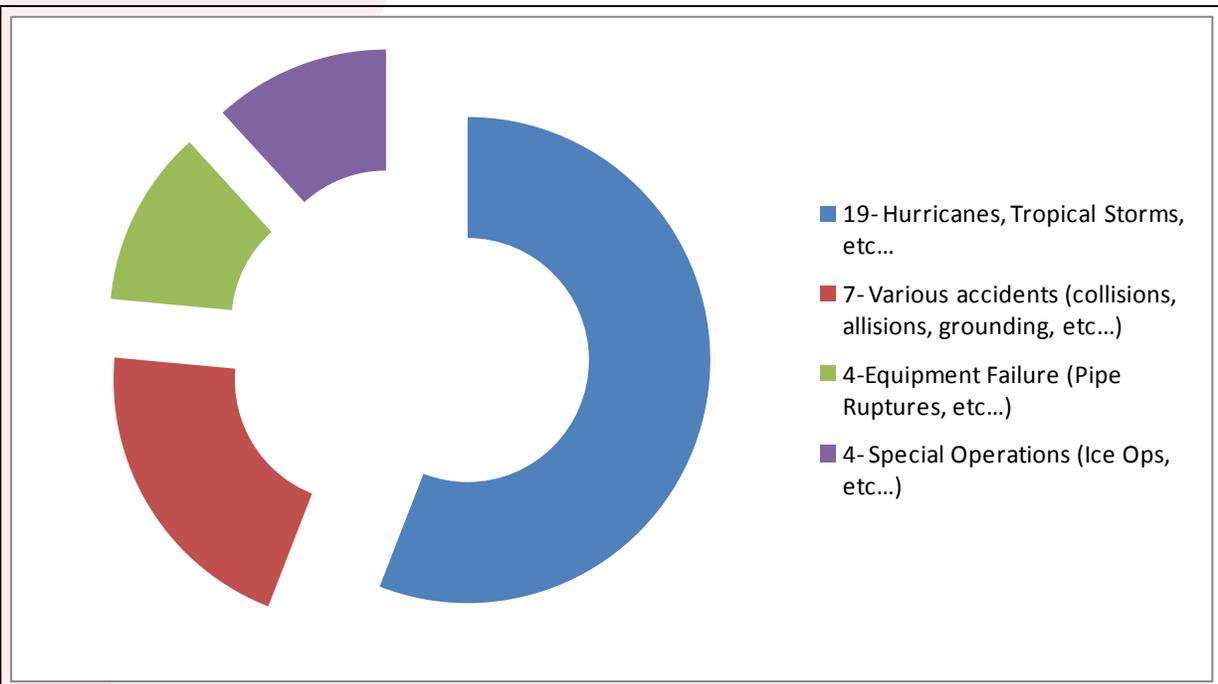
Trending Issues in Port Safety, Security, and Resilience

Common Asset Reporting Tool (CART)

CG-FAC continues to hear your comments and requests to improve the CART with the help of CG-6 (Asset Manager), CG-7 (Sponsor Representative), and the Operations Systems Center (OSC) (System Developer), ensuring that appropriate enhancements were completed. Enhancements completed in CY 2015 included:

1. Created an Essential Element of Information (EEI) for CG units to have for users to specify HURCON status;
2. Created additional EEI types including:
 - Port Area – MTS Essential Infrastructure
 - i. Petroleum Facility
 - ii. LNG/LPG Facility
 - iii. Chemical Facility
 - iv. Bulk Facility
 - v. Break-Bulk Facility
 - Waterway and Navigation Systems
 - i. Anchorages
3. Added two new methods to disseminate CART information to users – An Announcement feature and an E-mail Notification feature.

In 2015, there were a total of 34 events created in CART ranging from natural, accident, or equipment failure related disruptions.



What to Expect in 2016

- CG-FAC has purchased 22 iPads for Yorktown to use as a training tool in the Waterfront Facilities and Explosive Handling Supervisor courses. The intention is to assist the members attending the courses with using the devices in the field. Yorktown will take time to familiarize themselves with the devices prior to using them in class.
- Facility Security - A policy letter encouraging facilities to submit their FSP/VSP/ASP renewals to the Coast Guard 60 days prior to the expiration date will be signed and disseminated to the field in CY16. Also, the Breach of Security Instruction has been updated to include suspicious activity response. The instruction will be published mid-2016 and will address network security in addition to physical security incidents. Finally, be on the lookout for NVIC 03-03, Change 3 as well as an Alternative Security Plan NVIC in CY16.
- EHC Strategy - CG-FAC will be working with other offices to create an Implementation Working Group for the EHC Strategy. This working group will look to implement the four goals of the EHC Strategy including awareness, prevention, response, and recovery.
- Cyber - CG-FAC is working on several policy updates concerning cyber risk management. In cooperation with NIST, CG-FAC is drafting a Cyber Framework Implementation Guide for bulk liquid facilities. This will help facility operators identify the components of the NIST Cybersecurity Framework most applicable to their operations. CG-FAC is also developing a NVIC that will provide cyber risk management guidance to facility and vessel operators. CG-FAC will continue to support the Areas on conducting Cyber Awareness Training for CG Units.
- IMO— CG FAC will lead the U.S. delegation to the FAL committee at the International Maritime Organization to address various topics, including cyber risks for trade related information. CG-FAC will also attend the Marine Safety Committee of the IMO to address cyber risk management requirements for vessels.
- PSS Program - CG-FAC will work with FORCECOM to develop a Performance Support System for the PSS and PSSRs. Containers: CG-FAC is working on guidance for the implementation and enforcement of the update to SOLAS VI Regulation 2/6. This regulation will take affect 01 July 2016, and will mandate that all containers intended to be loaded onboard a SOLAS regulated vessel shall have a Verified Gross Mass prior to loading.
- Exercise requirements: CG-FAC is working on policy to clarify the definition for annual, and other time periods, as it is used in the 33 CFR 154 for exercise requirements.
- Pipeline testing: CG-FAC is updating current policy and incorporating that into a pipeline testing policy NVIC that will guidance on alternate testing methods.
- HOMEPORT— CG FAC is working with other Coast Guard Headquarters Offices to complete a long overdue technical refresh of Homeport. This update will improve

What to Expect in 2016

reliability and cyber security for the system and provide a better user interface.

Regulatory Projects:

- Consolidated Cruise Ship Security - The public comment period for this NPRM ended on June 1, 2015. The anticipated final rule publication date is in 2016. For more information please visit <http://www.regulations.gov/#!/home> and search “Consolidated Cruise Ship”.
- Seafarer’s Access to Maritime Facilities - The public comment period for this NPRM ended July 27, 2015. The anticipated final rule publication date is in 2016. For more information please visit <http://www.regulations.gov/#!/home> and search “Seafarers’ Access”.
- Transportation Worker Identification Credential (TWIC) Reader Requirements - The Final Rule is in final agency clearance.

Please refer to the DHS Unified Agenda for official anticipated dates of publication and status of the rulemaking projects. Keep in mind that this website is updated infrequently.

[http://www.reginfo.gov/public/do/eAgendaMain?
operation=OPERATION_GET_AGENCY_RULE_LIST¤tPub=true&agencyCd=1600](http://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST¤tPub=true&agencyCd=1600)

Office of Port and Facilities Compliance Contact List

Office Chief

Captain Andrew Tucci 202 372-1080

Domestic Ports (CG-FAC-1)

CDR Nick Wong 202-372-1107
Mr. Ryan Owens 202-372-1108
Ms. Etta Morgan 202-372-1120
Ms. Marilyn Small 202-372-1092

Port Resiliency/Recovery Branch

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

Critical Infrastructure (MTSR, Cyber Security, & PSS Training)

LCDR Josh Rose 202-372-1106
LT Josephine Long 202-372-1109
Mr. Robert Reimann 202-372-1146

Cargo and Facilities (CG-FAC-2)

CDR Jeff Morgan 202-372-1171
Mr. Jim Bull 202-372-1144

Facility Safety (explosive handling, containers, COAs)

LCDR Darwin Jenson 202-372-1130
LTJG Robert Bobuk 202-372-1114
MSTC Kevin Collins 202-372-1127
Mr. David Condino 202-372-1145

Facility Security (MTSA)

LCDR Jennifer Osburn 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
LT Cal Fless 202-372-1151

Strategic Planning / Development

CDR Brian McSorley 202-372-1131

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>