Waves on the Waterfront

CG-FAC, Office of Port and Facility Compliance

Safety, Security, and Stewardship

Volume 6
Issue 1

July 2017

Advances in Cyber Policy development – Your opportunity to provide feedback from the field

CAPT Ryan Manning

In an effort to move forward on the Coast Guard's Cyber Strategy priority of Protecting Infrastructure, CG-FAC has recently published policy documents that we need you to 'field test' as our operational subject matter experts at the Sectors, MSUs and MSDs. An updated Commandant Instruction Manual on Breach of Security and Suspicious Activity Investigation for MTSA Regulated Facilities and Vessels was published in late December and a recent Federal Register Notice was posted seeking comments on a draft Navigation and Vessel Inspection Circular (NVIC) on Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities.

The updated Commandant Instruction Manual is the culmination of work that began in early 2016, with major changes that included; Cyber-related definitions, reporting requirements for suspicious activity and guidance on cyber related events, including the new process/option to report to the Department of Homeland Security's National Cybersecurity & Communications Integration Center (NCCIC) rather than the National Response Center (NRC), which was solidified by a Service Level Agreement signed by our Assistant Commandant for Prevention Policy, RADM Thomas, along with the Directors of the NCCIC and NRC. I ask you, as our Coast Guard representatives in the field, to urge your regulated facilities to use this option for Cyber incident reporting. While the NRC is staffed with a great bunch of professionals, the NCCIC is uniquely staffed with Cyber professionals, ready to provide assistance and as their name implies, integrate cyber reporting across the whole of government.

(Continued on page 16)

SPECIAL ANNOUNCEMENTS

Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities

A draft Navigation and Vessel Inspection Circular on cyber risk management guidelines has been posted in the Federal Register here for review and comment.

Submit Your Articles

Do you have something you'd like to have published in the next edition of the Waves on the Water? Please send your articles to: ryan.f.owens@uscg.mil

Hail and Farewell

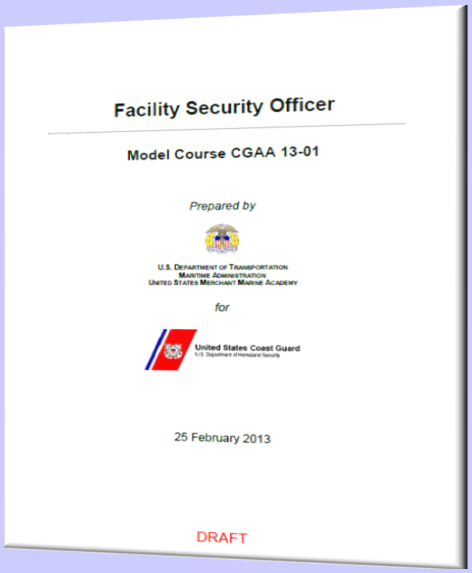
CG-FAC is pleased to welcome CDR Timothy Grant, LCDR Rachel Stryker , and LCDR Yamaris Barril to the FAC family.

We'd also like to say Fair Winds to CDR Nick Wong, LCDR Chris Pisares and Mrs.. Etta Morgan

Facility Security Officer Training…..
What's the Status?

LCDR Adam Cooley

The professionalism and hard work of waterfront facility and vessel owners and operators in supporting the requirements of the Maritime Transportation Security Act of 2002 (MTSA) have resulted in a more secure maritime environment. Looking at the past five years, the number of Facility Security Officer (FSO) related deficiencies averaged approximately 98 per year. This is down from the 196 per year average calculated for the first five years since the Coast Guard began enforcing MTSA. Reductions of these types of deficiencies can be attributed to many factors, including the ongoing development of a structured FSO training program.



The FSO voluntary training program has been on the Coast Guard Office of Port and Facility Compliance (CG-FAC) radar since MTSA was enacted and it continues to remain a primary topic of discussion. Section 109 of the MTSA charged the Secretary of Transportation with developing "standards and curriculum to allow for the training and certification of maritime security professionals." This initial effort was delegated to the Maritime Administration (MARAD) and the United States Merchant Marine Academy (USMMA) in 2004.

The work undertaken by MARAD and USMMA, and through cooperative efforts with the International Maritime Organization, maritime industry and other government agencies, resulted in the creation of a draft model course curriculum. In an effort to assist course providers charged with implementing the training provisions of MTSA, MARAD and the Coast Guard developed a voluntary program for maritime security training course certification. Another goal of this program was to help ensure those courses were best aligned to meet regulatory requirements. The full guidelines for the approval of training courses and programs are published in 46 CFR 10 Subpart D and supplemented by Navigation and Vessel Inspection Circular No. 03-14.

The Coast Guard is working to complete proposed regulations for FSO training and certification to meet the requirements of the 2010 Coast Guard Authorization Act, Section 821. In late 2012, CG-FAC hosted a public meeting at which industry provided comments on the draft model course curriculum. We are now working to incorporate the model course into a Notice of Proposed Rulemaking. The National Maritime Center (NMC) is the Coast Guard's premier credentialing service center for qualified mariners. Additionally, the NMC evaluates all requests for the approval of training courses and programs. A listing of all Coast Guard approved courses and providers are available on the NMC's website at: https://www.uscg.mil/nmc/default.asp.

Utilizing Coast Guard approved course providers for FSO and/or MTSA security related training is voluntary at this time; however, it's highly encouraged to help ensure FSOs and security personnel meet the training and knowledge requirements published in Title 33 Code of Federal Regulations part 105. The Coast Guard is confident that the current draft model course will reinforce core knowledge, understanding, and proficiency that must be possessed by FSOs in all U.S. facilities regulated under MTSA. The result of continued efforts will only strengthen the security of our nation's ports which ultimately will reduce the likelihood of a transportation security incident. For a copy of the current model FSO course, please visit: https://www.uscg.mil/hq/cg5/cg544/facilities.asp.

Long Island Sound After Hours Compliance Activities

Sector Long Island Sound After Hours Compliance Activities

Coast Guard Sector Long Island Sound is located in New Haven, Connecticut, and has an area of responsibility (AOR) that covers coastal Connecticut and New York along Long Island Sound, as well as portions of Long Island's south shore. This Sector and their subunit, Marine Safety Detachment (MSD) Coram, oversee regulation of 61waterfront facilities which includes bulk liquid oil and hazardous materials facilities, ferry terminals, public access, and mobile transfer facilities. Annually, Sector Long Island Sound and MSD Coram conduct approximately 130 facility inspections.

After identifying an egregious security violation at a facility during an early morning Port State Control exam, Sector Long Island Sound initiated a program they called "Operation Sleeping Guard" to conduct regular compliance inspections after normal working hours to ensure marine safety and security was maintained on waterfront facilities in their area of responsibility at all times. Like similar after hours compliance activities conducted in other areas of responsibility, these facility inspections were conducted by occasionally shifting facility inspectors work schedules, so additional resources were not needed.

The program identified numerous instances of non-compliance, helping to determine trends throughout the area of responsibility. When deficiencies were identified, on the spot training was conducted with facility personnel on the regulations and outreach was conducted after the fact to ensure facility management understood the applicability of regulations at all times. Ultimately, the program helped ensure compliance of facilities with regulations designed to help ensure port safety and security and closed vulnerabilities that may have existed prior to the initiation of the program.

While there is no requirement, it is recommended for other facility compliance divisions to consider conducting after hours activities to ensure port safety and security is maintained at all times. Likewise, facility owners and operators are encouraged to conduct internal audits of the implementation of their policies and procedures to ensure compliance at all times, not just when management or Coast Guard personnel are present on the facility.

No ID Checks or Screening at the Vessel or the Passenger Terminal? *What in the World ?*

Betty McMenemy

Yes - it happens and it is completely compliant with regulation. CG-FAC has gotten several calls regarding the "whys" of this process and how it can possibly be compliant. Following the requirements found in 33 CFR parts 104 & 105 this is how it happens. Let's start with the facility.

First, **33 CFR 105.106** discusses "Public access areas" and states:

(a) A facility serving ferries or passenger vessels certificated to carry more than 150 passengers, other than cruise ships, may designate an area within the facility as a public access area.
(b) A public access area is a defined space within a facility that is open to all persons and provides pedestrian access through the facility from public thoroughfares to the vessel.

Further**, 33 CFR 105.110** "Exemptions" adds:

(b) A public access area designated under §105.106 is exempt from the requirements for screening of persons, baggage, and personal effects and identification of persons in §105.255(c), (f)(2), (f)(3)*, (g)(1), (h)(1)and §105.285(a)(1).

The above cited CFR locations allow for facilities serving ferries or passenger vessels to designate a public access area that does not require ID checks or screening.

It is important to note, however, that **33 CFR 105.285** "Additional requirements – passenger and ferry facilities" states:

At all MARSEC levels, the owner or operator must ensure . . . the requirements of this part:
(5) In a facility with a public access area designated under §105.106, *provide sufficient security personnel to monitor all persons within the area.* (Emphasis added.)

In this instance, "monitoring" is a very important part of the passenger access area designation and management and should not be overlooked. Monitoring means "somebody ensuring proper conduct," "somebody who checks for incorrect or unfair conduct." When used as a verb it means "To observe and check the progress or quality of (something) over a period of time; keep under systematic review."

Some synonyms for monitoring are observe, watch, track, keep an eye on, keep under observation, keep watch on, keep under surveillance, surveil, record, note, oversee.

Although ID checks and screening according to the MARSEC Directive are exempt in public access areas, it seems pretty clear that it does not mean NO security. Having *enough* personnel means that the passengers within the designated area are monitored by security persons trained IAW §105.210 in a manner sufficient to observe whether any individual is engaged in activities that could likely threaten security.

What about the vessel? Look at **33 CFR 104.292**, which lists additional requirements for passenger vessels and ferries. §104.292(b) instructs, as an alternative to ID checks and screening requirements in

§104.265(f)(2), (f)(4) and (f)(9), the owner or operator of a passenger vessel or ferry may ensure security measures are implemented that include:

(b)(1) Searching selected areas prior to embarking passengers and prior to sailing; ***and***
(b)(2) Implementing one or more of the following:
(i) Performing routine security patrols;
(ii) Providing additional closed-circuit television to monitor passenger areas; or
(iii) Securing all non-passenger areas.

If the vessel follows these instructions they do not have to check IDs or screen passengers as they embark.

The Passenger Vessel Association (PVA) Alternative Security Program (ASP) gives their users the option of checking IDs and screening or using designated public access areas and/or utilizing the procedures outlined in §104.292. For facilities, the ASP requires monitoring or public access areas and *conducting screening as necessary*. The personnel monitoring these areas must be trained as required by §105.210 and, therefore, be able to recognize suspicious persons and require screening of any suspicious persons and packages.

*After TWIC rules were inserted into the CFR, locations of certain information changed and, to date, this has not been corrected. The cites in this article are correct.

Did you know the latest about . . .

MTSA/ISPS Policy Advisory Council (PAC) FAQs

PAC documents have been and continue to be relied upon by industry and the Coast Guard for facility maritime security waiver requests. A number of these documents state that, for a facility that meets all criteria listed in the PAC, "the Captain of the Port (COTP) can recommend to the District Commander, and the District Commander can approve the request." There are also several PAC documents that use the word "exemption" or "exempting" when referring to the facility waiver process. A MTSA waiver is not an exemption. Exemptions for facilities are found in 33 CFR 105.110 and for vessels in 104.110. Per guidance found in 105.130, requests for MTSA waivers shall be forwarded directly to Commandant (CG-FAC-2) attention Ms. Betty McMenemy.

To address these discrepancies, CG-FAC-2 recently issued COMDT (CG-FAC) memo 16611 of 16 NOV 16, titled "Clarification of PAC Document Guidance Regarding 33 CFR Part 105 Waivers and 33 CFR Part 154 Exemptions." This is also posted on CG-FAC-2 Portal page.

This clarification memorandum also included information about the authority for granting 33 CFR 154 exemptions as found in 33 CFR 154.108. Requests for 154 exemptions shall be forwarded through the chain of command to Commandant (CG-FAC-2) for review and action.

Please review this clarification memo if you have not already done so. For facility security-related issues, please contact Ms. Betty McMenemy at 202-372-1122. For facility safety-related issues please contact LCDR Dan McQuate at 202-372-1130.

https://cg.portal.uscg.mil/units/cgfac2/

Navigating the Hazards of a Working Waterfront Facility

LT Laura Gould

Recently a team of qualified Coast Guard container inspectors experienced a minor accident with a Government Vehicle (GV) at a waterfront facility. The container inspection team arrived at the facility and met with a facility representative who directed them to park the GV in a designated location on the working pier. This area was identified by the facility representative and marked with a caution cone adorned with an amber rotating light. After parking the GV in the designated area, the container inspection team began to remove equipment from the trunk when they observed a nearby gantry crane quickly move toward their location. The container inspection team members backed away from the path of the rapidly approaching gantry crane to a safe distance and observed the crane strike the GV prior to coming to a stop. The GV was not parked directly in the path of the gantry crane itself but the mechanical operating box on the crane extended beyond the width of the crane's front tires and side-swiped the parked GV. Prior to the gantry crane's movement toward the parked GV, the crane operator's booth was located on the opposite side of a four-high stack of containers. As the crane moved along the pier, it straddled the containers causing the operator to have limited visibility of the surrounding pier. The gantry crane is equipped with an automatic stop safety sensor located in the front of the crane but due to the position of the parked GV relative to the path of the crane the sensor did not engage to stop the crane. The crane has an emergency stop button on the mechanical operations box which was impacted when the mechanical box struck the GV. This caused the crane to stop moving. There were no injuries reported to Coast Guard members or facility employees. Estimated damage to the GV was approximately $2,000. No damage to the gantry crane was identified. A police report was filed and the appropriate notifications and MISHAP report were conducted by the unit. Additionally, an applicable safety stand down and general safety awareness training for operating on a waterfront facility was conducted for the benefit of unit personnel. The local MISHAP report instruction was also updated.

The best laid plans: In this incident, Coast Guard members identified their presence on a waterfront facility to the facility operator and established an area chosen by the facility representative to park the GV on the

pier. They used additional safety identification equipment (cone with a rotating amber light) to bring awareness to their location to people operating heavy equipment on the facility. They also parked the GV outside of the operational traffic lanes for the gantry crane which are painted on the ground in red and yellow stripes. Despite taking appropriate safety precautions, an accident occurred causing damage to the GV but resulted in no injuries to Coast Guard or facility personnel. The Coast Guard members stayed vigilant and aware of their surroundings while on the facility and were able to identify the hazard presented by the crane and moved to a safe distance. While the goal is to have a flawless safety record conducting Coast Guard missions, the potential consequences of accidents can be minimized by having sufficient training and qualifications, wearing the appropriate and required personal protective equipment (PPE) and remaining aware of surroundings at all times. Additionally, taking the time to discuss what went wrong and how a similar accident can be prevented in the future provides an opportunity to develop best practices and educate additional unit personnel. In this instance, established safety features were circumvented when the crane operator was not able to see the parked GV from the operation booth and the automatic stop sensors did not engage because the vehicle was not in the direct path of the crane. Simultaneously, the container inspection team maintained situational awareness and identified the impending hazard, removing themselves to a safe distance and preventing potential injuries.

Personnel are reminded that while on container yards and waterfront facilities, inspectors shall remain alert for moving vehicles or other container handling equipment to avoid being inadvertently struck. Heavy equipment operators on working waterfront facilities are often working in positions of limited visibility and will rely on safety equipment and operation within designated drive lanes to prevent accidents. Inspectors should make their presence known to the facility operators and work with the facility safety manager or other equivalent representatives to identify a safe working area on the facility. Coast Guard members should also analyze the designated working area for potential hazards and communicate with the facility representative if there are any concerns.

The safety of Coast Guard inspectors while performing their duties is of utmost importance and the standardization of inspection and safety procedures is a top priority. All container and waterfront facility inspections and the supervision of explosive outloads shall be conducted with caution, given the safety and health risks these activities present. As part of mission preparation and safety assessment, inspectors shall employ the concepts of Operational Risk Management as prescribed in The Operational Risk Management Instruction, COMDTINST 3500.3 (series), which can be accessed through the CGPortal: https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx. Additional operational guidance is provided in the MSM, the National Container Inspection Program Manual and TTP and various policy letters.

Lastly, job aids and reference materials enable inspectors to do their jobs accurately but can present a distraction while being used on a waterfront facility. Coast Guard members should make sure to find a safe location to look up information and have one team member remain on the lookout for unforeseen hazards. Focus on the task at hand is important for mission success but remember to be mindful and look out for yourself and your shipmate while working in hazardous conditions.

BRAVO ZULU to the inspectors in this article who ultimately stayed safe navigating the hazards of a working waterfront facility.

11/30/2016: Polar Code – An overview

The International Code for Ships Operating in Polar Waters, commonly known as the Polar Code, is a ship-focused code with specific provisions that enhance the design, operations, and equipment standards of vessels operating in Arctic and Antarctic waters. The Polar Code will enter into force on Jan. 1, 2017, and is divided into two Parts.

For more on this story, go to **http://mariners.coastguard.dodlive.mil/**

Maritime Bulk Liquid Transfer Cybersecurity "Profiles"

The Office of Port and Facility Compliance, the National Institute of Standards and Technology (NIST), and maritime industry stakeholders have developed a voluntary cybersecurity "Profile" for Maritime Bulk Liquid Transfer (MBLT) facilities. This Profile was released at the American Petroleum Institute's 11th Annual Cybersecurity Conference in Houston on November 10th.

The Profile implements the NIST Cybersecurity Framework, which was developed in 2014 to address and manage cybersecurity risk in a cost-effective way based on business needs and without placing additional regulatory requirements on businesses. The Profile is how organizations align the Framework's cybersecurity activities, outcomes, and informative references to organizational business requirements, risk tolerances, and resources. Through this industry-focused Profile, MBLT facilities are provided a pathway for integrating the Framework into organizational operations.

The Profile is the first of its kind for the maritime transportation sector and it is the result of the extensive collaboration between this office, the NIST's National Cybersecurity Center of Excellence (NCCoE), and industry stakeholders.

"Working with the Coast Guard to engage the oil and natural gas industry in creating this profile is a prime example of the collaboration that takes place at the NCCoE," said Don Tobin, senior security engineer at the NCCoE. "Organizations working in this critical mission area can leverage the profile to determine and reach their desired state of cybersecurity."

The Profile identifies and prioritizes the minimum subset of Framework subcategories relevant to MBLT facility operations, providing the flexibility to address subcategories in a systematic way that is relevant to their unique operations. The Profile pulls into one document the recommended cybersecurity safeguards and provides a starting point to review and adapt risk management processes. It outlines a desired minimum state of cybersecurity and provides the opportunity to plan for future business decisions.

"This first Cybersecurity Framework Profile for the maritime transportation sector is the culmination of hard work from industry stakeholders, the Coast Guard and NIST to provide guidance to the MBLT industry to adapt their risk management processes to include cyber risk management," said Capt. Ryan Manning, chief of the Office of Port and Facility Compliance. "While these profiles are voluntary in nature, I highly encourage industry to consider using them to achieve optimal cybersecurity for their respective organizations."

Cyber risk management in the maritime industry has become increasingly important with the evolution of cyber-dependent technologies in the past decade. The Coast Guard and the maritime industry have recognized the growing potential for cyber-based systems to impact bulk liquid and other elements of the Marine Transportation System. Operational technology now, more than ever, operates valves, pumps, sensors, control gates, cameras, and performs many other vital safety and security functions. Cyber attacks could lead to significant consequences. Cyber incidents, such as software problems, non-targeted malware, or operator error could have equally as serious of an impact. The potential consequences of a cyber attack or incident not only impact operations, but can also pose a threat to the Marine Transportation System as a whole.

"These facilities face inherent cybersecurity vulnerabilities and the Coast Guard hopes this profile will assist organizations with mitigating them, and provide a long-term process for developing an internal cyber risk management program," said Lt. Cmdr. Josephine Long, a marine safety expert in the Critical Infrastructure Branch within the Coast Guard's Office of Port & Facility Compliance.

According to Long, the Coast Guard anticipates working with the NCCoE to build four additional profiles; the next two will address passenger vessel and terminal operations, as well as mobile offshore drilling operations.

For more information, please view the entire Maritime Bulk Liquids Transfer Cybersecurity Framework Profile at http://www.uscg.mil/hq/cg5/cg544/docs/Maritime_BLT_CSF.pdf.

Cheniere Energy, LLC, Virginia Port Authority, Bridgeport and Port Jefferson Steamboat Company, and Port of Port Angeles Receive the Rear Admiral Richard E. Bennis Award for Excellence in Maritime Security

CAPT Randall S. Ogrydziak, Commanding Officer, Marine Safety Unit Port Arthur, presents the Rear Admiral Richard Bennis Award for Excellence in Maritime Security (Large Facility) to Mr. Aaron Stephenson, Cheniere Sabine Pass LNG Vice-President and General Manager. As the first terminal in the Continental US to export LNG, Cheniere's Sabine Pass Terminal is leading the way with their culture of security in identifying vulnerabilities and mitigating them, partnering with federal, state and local agencies to share best practices, improving security processes, reducing risk and preventing crime through environmental design.

Rear Adm. Meredith Austin, commander, Coast Guard 5th District, and Virginia Governor Terry McAuliffe present the 2015-2016 Rear Admiral Richard E. Bennis Award for Excellence in Maritime Security (Port Authority) to the Virginia Port Authority for outstanding achievements and contributions in safeguarding our nations Marine Transportation System, including port areas, adjacent waterways, coastal/shoreside areas, waterfront facilities, and other maritime critical infrastructure.

L-R Jeff Whitaker/2017 PVA President, Hudson River Cruises, USCG Rear Admiral Joseph Servidio Deputy. Commander, CG Atlantic Area, James McGuire/BPT-PJ Steamboat, Don Fromm/BPT-PJ Steamboat Company, Fred Hall/BPT-PJ Steamboat Company, Ron Panzero/King County Marine Division, 2017 Roger Murphy National Safety Award recipient, Kevin Suarez/Statue Cruises, 2017 Elizabeth Gedney Passenger Vessel Safety Award recipient, Matthew Gill/Statue Cruises, Margo Marks/2016 PVA President, Beaver Island Boat Company, and Bob Lawler/PVA Safety and Security Chairman, Entertainment Cruises.

CG-FAC Staff working with US International Partners in the Caribbean to Protect the Marine Environment from Pollution from Ships.

By David Condino

The USCG is the U.S. Government's point agency and Head of Delegation at the International Maritime Organization and implements and enforces international regulations for all ship's operating in US waters and all US ships on international voyages. IMO's International Convention for the Prevention of Pollution from Ships (MARPOL) requires all signers to the Convention to take a stewardship role aimed at ensuring compliance with regulations. Many countries party to MARPOL, especially small, less developed countries like our neighbors in the Wider Caribbean Region (WCR) face significant economic and governance challenges. One big governance challenge is creating and implementing national legislation that MARPOL requires. Economic challenges for ports and terminals include inadequate infrastructure to handle larger ships and more frequent port visits (and therefore more ship's waste) coupled with the lack of capacity in many Small Island Developing (SIDS) nations to manage even their own municipal waste much less operational waste from ships calling at their ports. The IMO recognized the need to take a regional approach in such areas and formalize recognition of Regional Arrangements (RA) and Regional Reception Facility Plans (RRFP) as a way to enhance compliance with MARPOL regulations by both ships and ports and terminals operating within a region.

The USCG works closely with our international trading partners to ensure ship owners and operators and port and terminal operators have the best available guidance and information on both ship and shore side waste management practices. This is especially important with our many trading partners to the south considering the extent of the US EEZ, and major US ports, in the Gulf of Mexico and the Atlantic and Caribbean coasts of Florida and the U.S. Territories in the WCR (Fig 1).

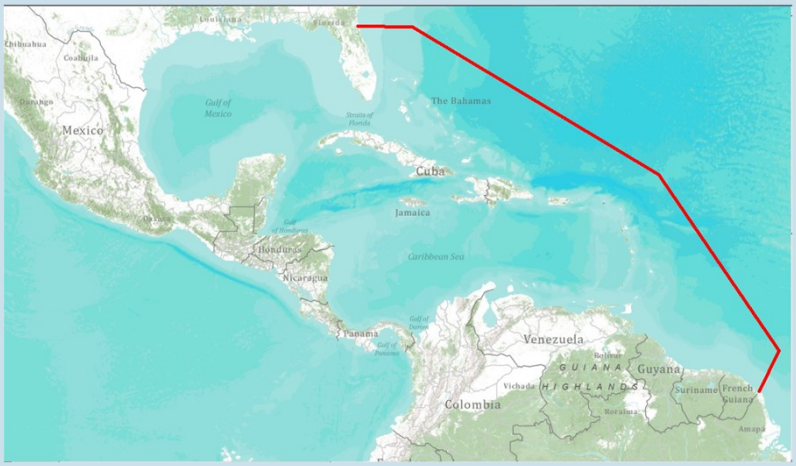


Fig 1, The Wider Caribbean Region (WCR) includes significant portions of the Gulf of Mexico and the Atlantic coast of Florida and the Areas around Puerto Rico and the US Virgin Islands in the Caribbean.

In 2013, under the IMO's Program of Technical Assistance, the USCG organized a three day workshop on MARPOL implementation and best practice waste management. With United Nations Environment Program (UNEP) funding assistance for travel, more than 30 delegates from Caribbean countries gathered in Ft. Lauderdale, Florida, to discuss 2013 updates to MARPOL regulations for ship discharges and ongoing challenges for ports and terminals in the WCR, and introduce the concept of regional waste management approaches as one possible solution that could help with MARPOL compliance.

Support for several workshops, including the 2013 Ft. Lauderdale workshop, on waste management in the WCR has come from the Regional Activity Centre/Regional Marine Pollution Emergency, Information and Training Center – Wider Caribbean Region (RAC/REMPEITC – Caribe), a regional unit of UNEP. The USCG HQ supports a Caribbean liaison officer billeted at RAC/REMPEITC – Caribe HQ in Curacao in the Dutch Caribbean Islands (currently CDR Keith Donohue), and he organized a 2015 Dutch sub-regional workshop in Aruba. At that meeting, several small Caribbean countries reported significant challenges in meeting MARPOL obligations and were using outdated and inaccurate PRF guidance and information. One outcome of the meeting in Aruba was a continued keen interest in the concept of RRFP for the WCR.

An RRFP would include participating states and identify all of the ports that would participate in the plan. While the IMO does not approve or disapprove of RA or RRFP for a particular region, it should be submitted for review by the Marine Environment

Protection Committee which may make recommendations aimed at improving the plan. Specific information is required for preparation of the plan and the IMO has published guidance on how to prepare an RRFP. The guidelines state that an RRFP should:

- Identify the region to be covered;
- Identify the nature of the unique circumstances that impact the ability to provide adequate port reception facilities in each SIDS within the region;
- In demonstrating the compelling need for a RA, explore alternatives, costed and assessed in terms of their environmental risk;
- Document how RA will contribute to efforts to improve the ability of SIDS to effectively fulfill its obligations under MARPOL, or to accede to MARPOL where a State is not already a Party;
- Identify and quantify the types of ships operating in each of these SIDS;
- Describe the overall voyage patterns of ships calling at ports in each of the SIDS;
- Describe all aspects of routing and voyage planning that might affect the amount of ship generated wastes and cargo residues on board ships arriving in each of the SIDS;
- Describe other relevant a*dditional considerations* that may influence the demand for port reception facilities in each of the SIDS;
- Identify which ports, if any, may be good candidates for R*egional Ships Waste Reception Centres (RSWRC)* in each of the SIDS;
- Identify *ports with limited facilities (PLF*), if any, in each of the SIDS; and
- Identify any potential options suited to the vessels calling at ports in these SIDS that will not encourage any illegal discharge into the sea.

The objective of the last workshop in Trinidad and Tobago in October 2016 was to further the work done at Ft. Lauderdale and Aruba and bring together experts from IMO and the region to a forum to discuss specifically the creation of an RRFP for SIDS in the WCR and set up a framework to accomplish specific tasks to:

- Obtain critical information needed to draft a RRFP for the Caribbean;
- Assess currently ongoing projects in waste management;
- Identify international and domestic shipping patterns;
- Create audit teams that will conduct gap analysis in ports identified as potential *Regional Ships Waste Reception Centers (RSWRCs);* and
- Identify key stakeholders for each of those Ports.

With these objectives in mind, work is progressing and plans are already underway for a follow-up meeting in 2017 to bring together data and audit teams along with identified stakeholders in the region including local and national authorities, industry groups, port operators, ship owners/operators, and waste management experts. The next steps will bring the entire region closer to being able to fully comply with MARPOL obligations while ensuring that ships don't contribute to pollution of pristine Caribbean waters. The USCG and the United States continue to lead the way as stewards of the ocean environment near and far from its shores. CG-FAC-2, Safety Branch, with full support of CG senior leadership, continues this work on the Coast Guard's core mission of protecting the environment.

Fig 2. Caribbean Nation Delegates and speakers from around the Caribbean and around the world meet in Trinidad and Tobago in October 2016. USCG CDR Keith Donohue, RAC/REMPIETC Liaison Officer, Curacoa is seated on the right, and David Condino, HQ USCG, CG -FAC, Washington is standing, third from left.

So, You Want to Go to Cuba by Boat…

By: LT Bradley Bergan and MSSD3 Daniel Sammons

In the wake of normalizing relations between the United States (U.S.) and Cuba, and following a substantial increase in vessels permitted to travel between the two countries, U.S. Coast Guard Sector Key West Prevention personnel have screened more than 800 vessels transiting to and from the Florida Keys and Cuba. The purpose of this screening process has been to educate vessel owners and operators and ensure vessels traveling to and from Cuba are in compliance with the wide range of safety, security, and vessel documentation requirements applicable to various vessel platforms. As a result of this enhanced vessel screening program, Sector Key West has also detected a handful of vessel operators in violation of federal statutes and regulations pertaining to vessels on international voyage. Suspension and Revocation (S&R) action was taken in one case where the operator of a yacht sailed to and from Cuba without a valid Certificate of Documentation (COD), Certificate of Inspection (COI), and required endorsements on the Merchant Mariner Credential (MMC). This mariner ultimately settled with the Coast Guard after a complaint was issued and is currently serving out a mitigated sanction on probation. Additionally, a Letter of Warning was issued in a second case where an operator took paying passengers to Cuba without a valid COD and six or less passengers for hire.

A marine safety information bulletin (MSIB) was published to the Key West Homeport page to expand outreach and education efforts to the public regarding international voyage requirements. Units are encouraged to share the linked MSIB and below information with operators planning to take passengers or freight for hire on an international voyage (e.g. Cuba):

What sorts of permits are needed to travel to Cuba? Vessel trips to Cuba are limited to authorized transactions outlined by the Treasury Department's Office of Foreign Assets Control and Commerce Department's Bureau of Industry and Securities. If you meet an authorized transaction criteria, you must also complete a U.S. Coast Guard "Application for Permit to Enter Cuban Territorial Seas" and submit it via fax to Seventh Coast Guard District at (305) 415-6800.

Are you taking passengers or freight for hire on this trip? If the answer is a definitive "no" then you are a recreational boater. If you are carrying passengers or freight for hire, you are a commercial operator. Recreational boaters are strongly encouraged to complete a full search of their vessels prior to departing Cuban waters to ensure that no unauthorized persons or goods are brought back to the U.S., and to ensure compliance with requirements of other Federal agencies, including U.S. Customs and Border Protection (CBP). Failure to do so may subject you to criminal or civil penalties, including vessel seizure.

What does a passenger for hire operation look like? "Passenger for hire" means a passenger for whom consideration is contributed as a condition of carriage. Consideration is defined in Section 2101 of Title 46, United States Code (USC) as an economic benefit, inducement, right, or profit including pecuniary payment accruing to an individual, person, or entity, but not including a **voluntary** sharing of the actual expenses of the voyage. Basically, if your vessel carries just one passenger, who provides anything more than a voluntary sharing of the cost of the trip, your vessel is operating as a passenger vessel. Passenger vessels can be uninspected passenger vessels (UPV) or inspected passenger vessels, depending on the total guests onboard. Six passengers or less and your vessel is considered a UPV, but that seventh passenger will require your vessel to be certificated by the Coast Guard. Vessels transporting passengers for hire between the U.S. and Cuba are subject to varied documentation, inspection, certification, and credentialing requirements.

What if I am bringing goods over to Cuba on my trip? Depending on what agency you are dealing with, the transportation of goods to and from the U.S. can become somewhat complicated, as most agencies have categories for various goods. The Coast Guard is particularly concerned with vessels transporting freight for hire. "Freight for hire" is defined as the "carriage of any goods, wares, or merchandise or any other freight for a valuable consideration whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel." Other agencies also have roles to play in freight for hire and transportation of goods. You, as a commercial operator, are strongly encouraged to reach out to your local CBP office to discuss your individual circumstances.

So, my boat is registered in the state of Florida, do I need to have any other form of registration? This depends on the tonnage and service of your vessel. A COD issued by the National Vessel Documentation Center and endorsed for the specific trade of the vessel is required to be maintained on board commercial vessels of at least five net tons in accordance with 46 CFR Part 67. Vessels subject to 46 CFR Part 67, operating commercially on international voyages, may require a "registry" endorsement. Vessels operating commercially within/between U.S. zones may also require a "coastwise" endorsement.

Does my boat need to be inspected by the Coast Guard? There are many scenarios which require commercial vessels to be inspected. Small Passenger Vessels (SPV) carrying more than six passengers, where at least one is for hire, are subject to inspection under 46 CFR Subchapter T and vessels carrying more than 12 passengers on an international voyage must comply with certain sections of the International Convention for the Safety of Life at Sea (SOLAS). Freight for hire vessels (more than 15 gross tons or certain hazardous materials-any tonnage) may also require inspection.

So, if I have taken my state boating safety course and printed out my identification card, am I ready to operate commercially? No. If you are carrying passengers or certain freight for hire you will be required to hold a Coast Guard issued MMC. The process for obtaining or renewing an MMC can be found on the National Maritime Center website at https://www.uscg.mil/nmc/. Mariners intending to operate commercial vessels internationally must have an MMC endorsed for international voyages.

I made sure I applied for and received my permits, had my vessel documented and inspected (if required), and hold the correct MMC, is that all there is to it? Almost. Commercial operators must submit advanced arrival notices in accordance with 33 CFR 160.212 and ensure notices are submitted within time requirements. In addition, if you are operating commercially, you need to comply with marine casualties reporting in 46 CFR Part 4. Certain marine casualties, such as serious marine incidents, may require chemical testing of individuals directly involved and employers must be aware of how to implement a chemical testing program in accordance with 46 CFR Part 16.

Are there other agency requirements to be aware of before operating commercially to Cuba? Vessel owners/operators are encouraged to contact municipal, county, state, and Federal agencies that regulate commercial vessel trade and operations, such as CBP, Centers for Disease Control, etc.

Are there penalties for not complying with certain standards or requirements? Failure to comply with federal requirements pertaining to commercial vessel operations could result in vessel delays or restrictions, monetary civil penalties, and/or the initiation of action against holders of MMCs.

If you have any questions about the information passed in this article, feel free to call one or both of the authors at (305) 292-7524 or (305) 292-8804.

Out of the Box and into Cyber Security Resiliency

Andrew Germann
Port Security Specialist
Sector Northern New England

For Port Security Specialists, the cyber threat environment continues to be extremely challenging. The limited amount of cyber security expertise at the field level is creating the need for out of the box thinking and the development of new relationships with our academic neighbors.

Four years ago, Sector Northern New England's cyber security program consisted of providing awareness material and a number of FEMA funded training courses throughout the year. We quickly realized this was not going to meet the Coast Guard's and the Sector's expectations of identifying and mitigating the rapidly changing threats and vulnerabilities within the cyber domain. Our strategy was simple; provide cyber security awareness and the available tools to combat cyber attacks to our entire maritime community and their supporting infrastructure. To accomplish this, we recognized we needed assistance from the people that live and breathe cyber security. The question was, where and how could we convince a select group of cyber security experts to join our program? We hit the jack pot with the University of Southern Maine (USM). They had just recently created the Maine Cyber Security Cluster (MCSC) Lab and were in the need of student projects.

We kicked off the new relationship by incorporating a cyber element in the 2012 AMSTEP Functional Exercise and all subsequent AMSTEP exercises thereafter. Concurrent with planning for the 2012 exercise, the USM MCSC students developed and delivered cyber security training to the Incident Management Team on how to identify cyber attacks and how to best avoid or mitigate such attacks. By the end of 2012, this mutually beneficial relationship had already exceeded our expectations.

Following the success of the 2012 AMSTEP exercise, it only made sense to bring the USM MCSC Lab Professors on board as full members of the Area Maritime Security-Executive Steering Committee (AMS-ESC) and the Cyber Security Working Group. The relationship blossomed and what followed was a stream of innovative projects that incorporated the latest technology.

One of our main priorities was educating the end user, i.e., the person sitting at his or her desk with the ability to open doors to critical systems and information for hackers and other nefarious actors. The USM MCSC students came through and developed a training course called "Evil at the Coffee Shop." The course took place in the MCSC Lab and participants experienced common cyber attacks in a safe environment learning how to identify them and methods to mitigate them. Sector NNE funds three courses a year and offers attendance to the maritime community and supporting organizations. To reach a broader audience, a portable closed network was developed that allows facility employees to experience the same training in their own environment tailored to industry specific programs they use every day. The first pilot program took place in 2016 and was tied to a facility's annual exercise.

Further, to identify and reduce open Wi-Fi vectors in Northern New England ports, the USM MCSC students used commercial off the shelf hardware and software to conduct port security Wi-Fi assessments, designed to identify open or poorly protected Wi-Fi connections to sensitive systems. Extensive coordination with the AMS-ESC and other industry partners was conducted to ensure the campaign was successfully executed. The participating organizations with vulnerabilities were privately notified and provided with information on how to protect their networks. To date, team USM MCSC and SNNE have completed assessments in two of our major ports and plans are to complete an assessment every few years in all our major ports.

In 2016, USM received funding from the Port Security Grant Program to develop a BetaPort. While still under development, the BetaPort will be a custom-configurable virtual machine-enabled environment used by port stakeholders to conduct cyber security network assessments and to identify risks and vulnerabilities. Once the BetaPort is completed, USM can customize this optional resource for port partners to simulate cyber attacks, allowing the user to ascertain vulnerabilities and experience how well their resiliency and recovery plans withstand cyber attacks.

In summary, fostering a culture of best practices in cyber security hygiene with the ability to build resiliency, security, and safety into this domain will have to go well beyond the capabilities of most Port Security Specialists; it is a venture that must be predicated on a non-traditional relationship and innovative thinking by combining conventional methods and relationships with experts in our own backyard that will bring the latest technology to bear in our cyber security campaign.

Program Note– Several offices within Coast Guard Headquarters are working to develop a job aid/process guide for this type of activity. This guidance is intended to save field units from reinventing the wheel, achieve a level of consistency, and keep the chain of command informed.

BRAVO ZULU!!

- After 44 years of continuous service to the United States Coast Guard, Mrs. Etta Morgan has decided to retire. Mrs. Morgan started with the United States Coast Guard in October of 1972 and her dedication has remained steady. Her dedication to her shipmates and her phenomenal work ethic will definitely be missed throughout the Coast Guard, especially in CG-FAC. Fair Winds, Mrs. Morgan!

- LCDR Chris Pisares retired from the Coast Guard this July after 20 years of Active Duty. His devotion to duty and positive attitude will be missed in FAC. Good luck in your future endeavors, Chris!

- Mr. Robert Reimann has been appointed as an Alternate Designated Federal Official (ADFO) by CG-ENG to the Chemical Transportation Advisory Committee (CTAC) to lead the Hazardous Cargo Transportation Security Subcommittee (HCTSS). This appointment increases coordination between the CTAC and CG-FAC to more effectively work with industry on security concerns stemming from the transportation of especially hazardous cargoes.

- Kudos to Ms. Betty McMenemy (CG-FAC-2) and LT John Santorum (CG-PSA-2) in spending their valuable free time to volunteer with Thrive DC. They assisted Thrive staff to help prepare food, set up, and, serve the less fortunate in the DC area.

Founded in 1979, Thrive DC works to prevent and end homelessness in Washington, DC, by providing vulnerable people with a wide range of services to help stabilize their lives. Thrive DC has grown to be a comprehensive, professionally staffed, bilingual organization serving more than 2,000 men, women, and children each year. If you are interested in volunteering, please contact YN3 Aymee Zimmer or go to https://www/thrivedc.org/

Public Access Facilities—Unveiled

There is an old, but excellent, saying that touts, "A picture is worth a thousand words." I am happy to tell you that Chris Weiller of D7, Miami, put that adage to good use – and we are the beneficiaries.

At some time or another, everyone has had questions surrounding Public Access Facilities (PAF) – "what is and what isn't" a PAF being the main source of queries. Chris took the time to research and assemble an album of various types of piers to which vessels could moor to embark/disembark passengers. This job aid should help resolve some of those uncertain situations. Chris also added that if anyone has additional examples they'd like included - please email him.

The PAF job aid has been placed on CG Portal, FAC-2 home page and is available for reference.

Updated Breach of Security & Suspicious Activity Reporting Procedures

An owner or operator of a vessel or facility that is required to maintain an approved security plan in accordance with parts 104, 105 or 106 of Title 33, Code of Federal Regulations, Subchapter H, shall, without delay, report activities that may result in a transportation security incident (TSI) to the National Response Center (NRC), including breaches of security and suspicious activity.

The Coast Guard recently published 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 (COTP), Area Maritime Security Committees (AMSC) 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.

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 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 will document the report, evaluate it against current operations, provide technical assistance if requested and appropriate, and pass the collected information to the NRC. Information sharing between NCCIC and the NRC, which may contain sensitive security information, will be protected in accordance with 46 CFR 1520. The CG-5P Policy Letter 08-16 will be distributed by electronic means only and is available 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 .

(Continued from page 1)

The comment period for the draft NVIC ends 11 September 2017, and I'd ask not only for you to review with a critical eye as a Facility Inspector or Port Security Specialist, but also to seek feedback from the facilities in your AOR. While the comment period for this NVIC is limited to 60 days, this policy development is an evolution, so we will need to be continually informed as to the current 'state of cyber risk readiness' our regulated facilities are at. While it may not be an inspection item in your MTSA Facility Compliance Guide yet, take the opportunity to engage FSOs and Ops Managers while conducting your annual and spot check inspections to have the discussion about how their company is addressing cyber. You might be surprised at how developed some segments of the maritime industry are related to their Cyber Risk Management Policies & Programs.

Finally, both of these policy documents were the collaborative work that included input from HQ, Area and District Staff elements, and I'd ask you help further inform all of us from your perspective in the field. Thank you for all that you do, stay safe.

Office of Port and Facilities Compliance
Contact List

Office Chief	
Captain Ryan Manning	202-372-1080
Domestic Ports (CG-FAC-1)	
CDR Timothy Grant	202-372-1107
Mr. Ryan Owens	202-372-1108
Ms. Marilynn Small	202-372-1092
Port Resiliency/Recovery Branch	
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 (MTSR, Cyber, & PSS Training)	
LCDR Josephine Long	202-372-1109
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
LCDR Yamaris Barril	202-372-1151
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
LT Angela Alonso	202-372-1116
USCG TWIC Help Desk	1-877-687-2243; **option #1** TWIC.HQ@uscg.mil

CG-FAC Links

www:	http://www.uscg.mil/hq/cg5/cg544/default.asp
Portal:	https://cgportal2.uscg.mil/units/cgfac2/SitePages/Home.aspx
Homeport:	Homeport> Mission> Maritime Security or Ports and Waterways
TWIC (Portal):	https://cgportal2.uscg.mil/communities/twic-discussion/SitePages/Home.aspx