



SPECIAL ANNOUNCEMENTS

BRAVO ZULU!

Sector San Francisco expertly documented a TWIC confiscation. While conducting an unannounced security spot check, Sector regulatory personnel confiscated the TWIC. See MISLE Activity #5120052 .

In addition, while conducting an inspection, Sector Guam confiscated a TWIC due to card appearing on the CCL. See MISLE Activity #5081922.

Feedback

How can we improve Waves on the Waterfront? Would you like to see more articles from the field? More technical articles? More policy driven articles?

We welcome any suggestions! Please submit comments to Mr. Ryan Owens at:

Ryan.F.Owens@uscg.mil.

Waves on the Waterfront

CG-FAC, Office of Port and Facility Compliance
Safety, Security, and Stewardship

Volume 4
Issue 3



June 2015

Questions from the Field

The following is a new feature in Waves on the Waterfront that we hope to provide on a regular basis. Input from the field in the form of practical questions on how to make our enforcement programs work in view of real world challenges at the unit level (where the work of implementing policies that are written here at HQ gets done) is essential to the process of ensuring that regulatory, policy and program guidance is practical, user friendly and meets the needs of our inspection and prevention field personnel.

LTJG Inyang, MSU Port Arthur, recently prompted the following Q and A from CG-FAC-2 Safety Branch Staff regarding the MARPOL Certificates of Adequacy (COA).

LTJG Inyang writes,

“I wanted some clarification on Certificate of Adequacy (COA) as it pertains to the date of issuance of a renewal certificate. If an original certificate expired while the COTP was reviewing their renewal request, can the COTP use the date the review was completed or can the COTP revert back to the date the original certificate expired i.e. original COA expired 3Feb15 and review was completed 8May15? Is there a drop dead date for the COA?”

The regulations in 33 Code of Federal Regulation (CFR) 158.140 and 160 talks about applying for a COA and issuance of the COA. It states that each COA remains valid for a period of five years or until suspended, revoked; or the regulations no longer apply to the reception facility.

There is limited to no guidance on the renewal of the COA. COMDTINST 16450.27,29,31 does give some guidance but it is not specific to the reissuance of the certificate. It states that because the COA does not have any time limit for reissuance and remains valid until suspended or revoked, the COTP must be sure that the reception facilities are adequate prior to issuance. Also, there is the option to issue an interim COA letter mainly to give the COTP flexibility in scheduling reception facility inspections to meet operational commitments while at the same time permitting the terminals and ports that have satisfied all requirements, except for the inspection of their reception facility, to conduct normal operations. However, COTPs shall issue an Interim Letter COA only if the COTP is satisfied that the

Continued on Page 8

The Maritime Sector Coordinating Counsel and You

by Mr. Ryan Owens

Voluntary collaboration between private sector owners and operators (including their partner associations, vendors, and others) and their government counterparts is the primary mechanism for advancing collective action toward national critical infrastructure security and resilience. In a world in which reliance on critical infrastructure are shared by industry and government and where industry may be on the front lines of national defense, such as in a cyber attack, a sustainable partnership must be developed to address both public and private perspectives.

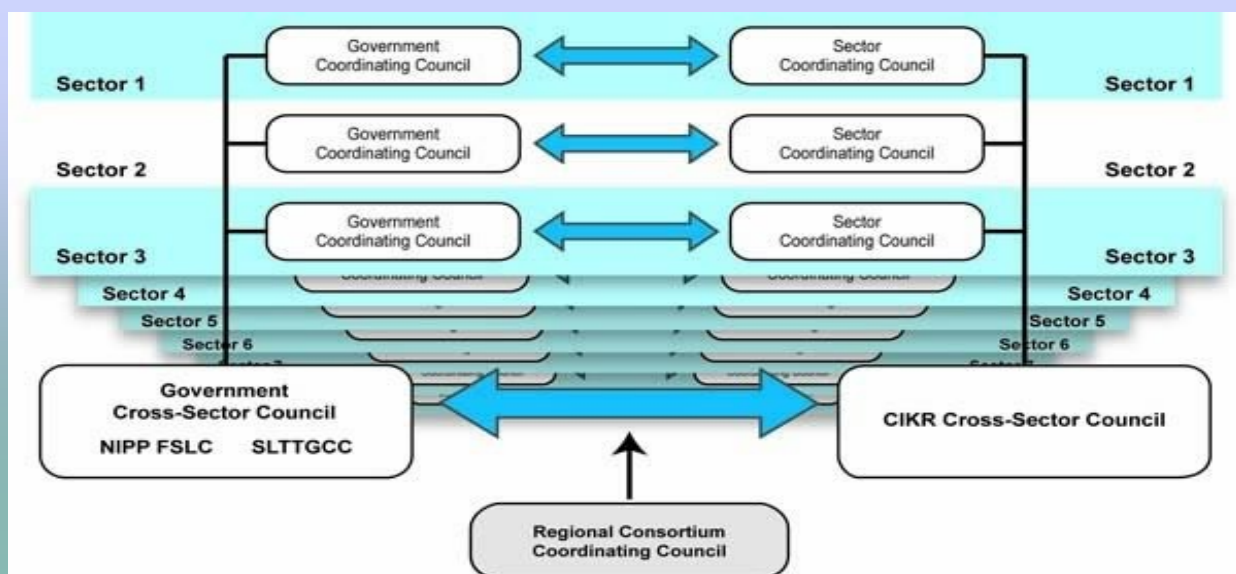
Traditionally, the Coast Guard has worked closely with their private sector partners through various mechanisms including: Federal Advisory Committees, Harbor Safety Committees, Area Maritime Security Committees (AMSCs), and direct involvement with industry advocacy organizations. The National Infrastructure Protection Plan envisions a similar partnership model through the coordination between Government Coordination Councils (a group made up of various Federal Stakeholders) and corresponding Sector Coordinating Councils (SCC)

The SCCs are self-organized, self-run, and self-governed, with a spokesperson designated by the

membership. Specific membership will vary from critical infrastructure (CI) sector to sector, reflecting the unique composition of each CI sector; however, membership should be representative of a broad base of owners, operators, associations, and other entities—both large and small—within a CI sector.

The primary functions of an SCC include the following:

- Represent a primary point of entry for government into the sector for addressing the entire range of critical infrastructure protection activities and issues for that sector;
- Serve as a strategic communications and coordination mechanism between critical infrastructure owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support the information-sharing capabilities and mechanisms that are most appropriate for the sector;



- Facilitate inclusive organization and coordination of the sector's policy development regarding critical infrastructure protection planning and preparedness, exercises and training, public awareness, and associated plan implementation activities and requirements; and
- Advise on the integration of federal, state, local, and regional planning with private-sector initiatives; and Provide input to the government on sector research and development efforts and requirements.

The SCCs are encouraged to participate in efforts to develop voluntary consensus standards to ensure that sector perspectives are included in standards that affect critical infrastructure protection. It is important to note that participation is completely voluntary and not associated with the AMSCs roles and responsibilities.

So, what's in it for members? As mentioned, the SCCs are self-organized, self-run, and self-governed. The membership take ownership in setting the agenda and identifying issues that they feel are important to the sector. An SCC can help address a wide range of persistent challenges without Federal oversight; for example, information sharing and coordinating lessons learned and best practices. It also allows members to be part of the discussion in the development of future maritime security policy. Further, once approved by the Department of Homeland Security, an SCC is considered an organization under the Critical Infrastructure Protection Advisory Council (CIPAC) and facilitate interaction between government representatives at the federal, state, local, and tribal levels and representatives from the community of CI owners and operators in each critical infrastructure sector to conduct deliberations and form consensus positions to assist the Federal Government.

Currently, the Maritime Transportation Sector does have an active GCC but it does not have an SCC, something the Coast Guard would like to see change. A vibrant SCC would go a long way in helping shape what cyber security in the maritime environment will look like as well as assisting in the development of the Transportation Sector's Sector Specific Plan (in

support of the National Infrastructure Protection Plan) and the current efforts underway to refresh the National Preparedness Goal. If you or your organization is interested in spearheading the effort to create a maritime SCC, please contact Mr. Ryan F. Owens at 202-302-6565 or ryan.f.owens@uscg.mil.

<http://www.dhs.gov/critical-infrastructure-partnership-advisory-council>

Hurricane Preparedness 2015

Hurricane Season is right around the corner! To prepare Coast Guard personnel and our private sector partners for the possible hardships brought forth by such ravaging storms, Coast Guard commands across the country are revising contingency plans, executing hurricane exercises, performing training, etc. These planning activities are necessary to ensure Coast Guard personnel and their families have the tools and information necessary to successfully mitigate the many ill effects these storms can cause. CG -FAC further recommends that units review their CART information and make sure their MTSRU and salvage plans are up to date.

Additionally, A key component as it relates to hurricane preparedness is ensuring information can be effectively communicated prior to, during, and post event to the masses. To that end, it's a prudent measure to ensure that the mechanisms for communicating with port partners have been tested and staff have been trained on their use. As a reminder, The Alert Warning System (AWS) Mobile App has been approved to for use by CG personnel and port partners. The AWS mobile app allows AWS alert recipients an easy and efficient means to receive and respond to AWS alerts. Instructions for downloading the AWS mobile app can be found in the news section <https://homeport.uscg.mil>

CG-FAC Roadshow Update

by LCDR Jennifer Osburn

Thanks to all of your great communication and cooperation, CG-FAC has been able to start conducting its roadshow workshops. The purpose of these roadshows is to continue effectively corroborating with Areas, Districts, and field units in addition to our bi-annual all hands workshops, and is intended for both facility/container inspectors and PSSs. Our goal is to share best practices and discuss area specific issues and challenges, in addition to providing requested training and regulatory updates. We are also making ourselves available to attend exercises or meetings (i.e. AMSC, Industry Day, etc.) as our schedule allows.

CG-FAC has provided Areas and Districts with our draft baseline agenda and asked that it be sent out to field units to provide feedback. These roadshows are for you, therefore we have requested that you help build out the topics and training for your area. This has been very helpful to tailor each workshop accordingly. So far we have visited units in Districts 14, 8, and 11 with great results. The remaining schedule is as follows:

D17 – June 9th in Juneau and June 11th in Anchorage

D7 – July 21st in Jacksonville and July 23rd in Miami

D5 – Aug 18th in Portsmouth

D13 – Aug 20th – 21st in Seattle

D1 – TBD

D9 – Sep 16th in Cleveland

One thing we have felt is beneficial is for units to provide CG-FAC with any specific questions and/or local challenges in advance so we can research and prepare to discuss during the workshop. If you have questions about these roadshows, please feel free to contact our office.



Port of Honolulu



Port of Houston



D11 Workshop

Unique procedures during Explosive Handling Operations in your AOR

Tired of wondering, “Is this policy still in affect?” “Has Headquarters released something new and I missed it?” Wonder no more! A new Explosive Handling Supervisor (EHS) Instruction has been created and is in the process of review. What I have done is I collected all of the old policies, directives, and COMDTINSTs that I could find and consolidated them into one. Ok, you can stop cheering now; it is still in the process of review and could take a while for concurrent clearance. In the meantime, I charge your office, if you choose to accept, to send me feedback on unique operations that your COTP allows under their authority, and you would like to have addressed in the guidance. For example, a unit allows a larger container/magazine of explosives to be emptied into two smaller containers/magazines while at the waterfront facility before being transported. There are safety precautions and other stipulations in place while this operation occurs, but this is unique and may be in full compliance under the COTP Authority. This specific operation has been addressed in the new guidelines. I’m not going to promise all of your feedback will be addressed, but I will do my best. Please send your unique operations to MSTC Kevin W. Collins at Kevin.w.collins@uscg.mil with the Subject line as EHS Operations at Sector/MSU/MSD...

TWIC Delays

In recent months the Coast Guard has received notification from the field of significant delays in the processing of TWIC enrollments. Currently some TWIC applicants are experiencing delays of more than 60 days to receive their TWIC. TSA regrets any inconvenience or difficulty this may be causing, and are working diligently to reduce the time it takes to process all TWIC applications. The delays apply to applications that involve a criminal record or an immigration status that must be verified, although some others may also experience a delay.

In view of these potential delays, TSA strongly encourages anyone needing a TWIC to enroll at least 10 to 12 weeks prior to when the card will be required to avoid inconvenience or interruption in accessing maritime facilities or executing the privileges of a U.S. Coast Guard mariner’s credential.

If you have additional questions or concerns please contact the TWIC help desk at 1-877-MTSA-AID (1-877-687-2243; Option 1) or at uscg-twic-helpdesk@uscg.mil



Questions from the Field (cont)

terminal's COA Application is complete and accurate, the conditions for adequacy are met, and EPA consultation requirements are completed. This guidance is all good for the initial issuance of the COA but may not address the reissuance of the COA as far as the procedures to follow if the COTP review period is outside the validity period of the existing COA of the facility.

Another issue is: can the facility continue to operate after the expiration of their current COA while the COTP is reviewing their renewal request or do they have to suspend any waste reception from vessels until the review is complete? “

CG-FAC-2, Safety Branch, response to LTJG Inyang,

LTJG Inyang brings up some very important issues, and while there is guidance (MSG, NVIC, policy letters, job aids) that tries to clarify some of these issues, our regulatory and policy processes don't always keep up with the fast pace of changes in MARPOL and even changes that Congress makes in the implementing Acts.

Since the COMDTINSTs are a bit dated and generally only cover the Application/Issuance of COA's, let's stay with the current regulations at 33 CFR 158 which implement MARPOL in accordance with the Act to Prevent Pollution from Ships (APPS) (33 U.S.C. 1901 et seq.)

According to 33 CFR 158.160 a COA expires 5 years from date of issue as shown on the COA. Since a COA is no longer valid after the expiration date, the port or terminal may not technically continue to receive ships. Further, authority is granted to a COTP to deny entry of ships to that port or terminal if it does not have a valid COA. (See 158.130, Delegation of Authority to COTP, and 158.135, COA applicability). Therefore, it behooves ports and terminals falling under applicability requirements to apply to the COTP to renew their COA in plenty of time to receive a new certificate prior to the expiration date.

However, 33 CFR 158.160 (Waivers and Alternatives), gives the COTP some latitude in granting a waiver to the requirements for issuing COA under Part 158. Hypothetically, if a port or terminal operator provides in writing an explanation why it was unreasonable or impracticable to renew the COA in a timely manner and proposes an alternative (e.g. submits the application, albeit late); and if the COTP agrees, then the COTP could likely issue a written waiver for the port or terminal to continue operations if, and only if, the port or terminal could in any event meet all the requirements in MARPOL for reception facilities. The waiver should be in writing and should be attached to the original COA.

The COTP may not issue a COA without first inspecting the facility. This is a requirement in APPS (33 U.S.C. 1905). Coast Guard HQ has issued message guidance to field units on expiration dates and phase out of original COAs without expiration dates, even prior to getting it into the regulation. This process should have been completed some time ago with all ports and terminals in the US applying for and receiving a new or renewed 5-year COA (following an inspection and after the USCG consulted with local EPA or other relevant agency, where required). A MARPOL inspection checklist is available on the CG-FAC-2 portal website: (<https://cgportal2.uscg.mil/units/cgfac2/SitePages/Home.aspx>).

We agree that the COMDTINSTs need to be updated; they were originally written when there was no expiration date. Now that there is a requirement for an expiration date, facilities should submit an application for renewal in a timely manner, and the COTP should reach-out to port and terminal operators within their AOR to ensure that they are aware of the COA requirements. The message guidance from HQ states as much. Use of "Interim COA letters" may not be a good precedent to set, given there is no mention in the CFR or in APPS and any use of 33 CFR 158.150 waiver process should only be on a case-by-case basis.

As to your last question concerning operating after the expiration date of their current COA. One might ask a similar question regarding mariner licenses: Would we let a mariner sail on an expired License/MMD? Once an application is received (sufficiently in advance of the expiration date which is the port or terminal operator's responsibility) the COTP should endeavor to complete the inspection and review process in a timely manner to prevent a lapse in compliance with US MARPOL regulations.

Is it a Waiver or an Exemption?

by Ms. Betty McMenemy

Many of us use the words “waiver” and “exemption” interchangeably. Actually, they do not mean the same thing. Applying for and receiving a waiver from Commandant allows a MTSA-regulated vessel or facility to continue to operate without having to implement some or all of the requirements found in 33 CFR 104 or 105. A regulated facility or vessel, based on their operations or on published Coast Guard policy, may not have to submit a Facility/Vessel Security Plan to the appropriate plan approval authority. Receiving a waiver means that, according to Subchapter H, the rule is applicable to the facility or vessel but the Commandant, with input from Sector, District, and Area has concluded that allowing the facility or vessel to continue to operate without a security plan does not compromise security.

33 CFR 104.130 – Because of their configuration and operations, vessels do not send many **waiver** requests to Headquarters. The most common requests received are from regulated vessels wishing to moor at non-regulated facilities. (The vessel is actually making the request on behalf of the facility.) In some cases the “facility” is a company or back yard dock. By regulation these requests must come to Headquarters, but are immediately forwarded to the cognizant COTP for decision. We have also received requests for TWIC waivers for summer workers (usually teenagers) or for some students at maritime schools who are not planning on going to sea but who nevertheless must spend time on a vessel during their school years.

33 CFR 105.130 – 33 CFR 105 is applicable to many facilities based on the cargo they transfer. As you know, there are many commodities that the Coast Guard Hazardous Materials Standards Branch has said are not likely to cause or be involved in a Transportation Security Incident (TSI). Some examples of those materials are: asphalt, drilling mud, charcoal, coal, sawdust. There are more cargos that fall into this category and they can be found in the Policy Advisory Council (PAC) documents available on the non-secure side of Homeport. These PAC documents also contain operational circumstances under which a waiver may be granted at the COTPs discretion.

Another often requested 105 waiver comes from small 33 CFR 154 regulated facilities fueling small vessels.

Based on operations, Subchapter H as described in 33 CFR 104.105 or 105.105, *IS* applicable to a facility or vessel requesting a waiver.

An **exemption** means that regardless of operations a particular vessel or facility type is not required to submit a Vessel or Facility Security Plan to the Coast Guard.

33 CFR 104.110 – MTSA rules do not apply to warships, naval auxiliaries, or other vessels owned or operated by a government and used only on government non-commercial service. They are exempt. Laid up, dismantled or out of commission vessels are also exempt from 33 CFR 104. This rule also impacts U.S. flagged Great Lakes vessels during the ice season.

33 CFR 105.110 – This section lists a number of facilities that do not have to comply with some or all of the MTSA associated regulations. Barge fleeting facilities and public access areas are exempt from some of the requirements of 33 CFR 105. General shipyards are exempt under specified conditions and Public Access Facilities may be exempt. For more information on facility exemptions see 33 CFR 105.110.

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. Marilynn Small 202-372-1092

Port Resiliency/Recovery Branch

LCDR Scott White 202-372-1116
Mr. Rogers Henderson 202-372-1105
Mr. Chris Dougherty 202-372-1157

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

LCDR Josh Rose 202-372-1106
LT Josephine Long 202-372-1109
Mr. Geoff White 202-372-1141
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
MSTC Kevin Collins 202-372-1127
Mr. David Condino 202-372-1145

Facility Security (MTSA)

LCDR Brian McSorley 202-372-1131
LCDR Jennifer Osburn 202-372-1132
Mr. Casey Johnson 202-372-1134
Ms. Betty McMenemy 202-372-1122

TWIC Implementation

LCDR Brett Thompson 202-372-1136
LT Bill Gasperetti 202-372-1139

Security Standards (Regulation Development)

LCDR Kevin McDonald 202-372-1168
LT Mason Wilcox 202-372-1123

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/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>