



SPECIAL ANNOUNCEMENTS

LGC NCOE Field Notice 01-2015 was released, and shares helpful recommendations, best practices and lessons observed during LNG bunkering operations. <http://www.uscg.mil/hq/cg5/lgcncoe/docs/LNG%20Bunkering%20Job%20Aid.pdf>. For questions or concerns please contact lgcncoe@uscg.mil.

BRAVO ZULU to Sector San Diego for their comprehensive and noteworthy Port Operating Plan. The plan outlines coordinated local, state, federal, and private sector activities, consolidates procedures that support reopening, clarifies roles and responsibilities of maritime stakeholders, and establishes clear lines of authority.
Job Well Done!

Feedback

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 5
Issue 1



February 2016

Homeport 2.0

The United States Coast Guard (USCG) Homeport Internet Portal (HIP) was established in 2005 to facilitate compliance with the requirements set forth in the Maritime Transportation Security Act (MTSA) of 2002, by providing secure information dissemination, advanced collaboration, electronic submission and approval for vessel and facility security plans, and complex electronic and telecommunication notification capabilities.

Since its inception, HIP has been expanded to provide additional support such as Transportation Worker Identification Card New Hire; Electronic Vessel Response Plan; Marine Event Permit Process; Port Status Indicator; Merchant Mariner Licensing and Documentation; Marine Training and Assessment Data (training documentation); Merchant Mariner Certificate; Sea Service Calculator; Merchant Mariner Verification of Certificates; and Merchant Mariner Credential Survey

HIP is at the end of its lifecycle, and an upgrade to Homeport 2.0 is required to keep pace with technological advancements. These changes will not only result in an all around better user experience, but information stored in the Homeport will be more secure.

The Coast Guard will launch Homeport 2.0 in the late spring/early summer timeframe in order to provide a better user experience and improve the security of user information. Homeport 2.0 will function the same as Legacy Homeport, although users may notice some cosmetic differences. Upgrades will include fewer site navigation menus and more efficient and secure search functions.

A complete list of application-specific contacts can be found in the Homeport 2.0 Application Points of Contact document located on the project site <http://www.uscg.mil/hq/cg5/cg544/homeport%202-0.asp>.

I saw something; I am saying something... is this worth it; what's done about it?

By LT Callan Fless

ANYTHING out of the normal operations can and should be looked into. Whether it is a situation that needs FBI (Federal Bureau of Investigations) and HSI (Homeland Security Investigations) involved due to indications of a terrorism nexus or reporting people taking pictures near a waterfront facility to American Waterways Watch (AWW) (Coast Guard-sponsored nationwide program that helps prevent acts of terrorism and other illegal activity that jeopardize maritime homeland security by educating and training members of the maritime and recreational boating organizations, as well as the boating public, to recognize and report suspicious activity to appropriate authorities <http://americaswaterwaywatch.uscg.mil/home.html>).

In a recent USCG real life situation (1), people taking pictures were questioned by local law enforcement, which recognized a need for escalation. The FBI was called in to investigate further and determined the people were from an Asian country and smuggled into the US through a secondary country via a known smuggling ring. Their phones/cameras were taken and are reviewed for content. They were deported after the interviews were completed, however, nothing in the interviews/biometrics raised terrorism concerns/links at conclusion of the investigation. In another recent USCG real life situation (2), people taking pictures were questioned by the Security Guard. The people asked how much money the Guard would take to allow them access to the pier to take pictures of the cruise ship. The Guard called the Security Supervisor over to speak with the people, but the people became agitated and departed in a rental car. The well dressed people claimed to be visiting from a South American country, and spoke Spanish and English in front of the Guard. The Guard also overheard them speak a different language when they spoke to each other, which he thought resembled Arabic. Although not detained/apprehended for further questioning, the FBI is investigating surveillance tapes.

These situations are all too common and unfortunately can easily go unnoticed or unchallenged. The two scenarios above are highlighted to demonstrate that even the most simple situations can hide some complex details under the surface. IAW 33 CFR 101.305 Reporting, Facilities are required to contact the NRC and DHS is encouraging private citizens to contact local law enforcement via 911. Be mindful of the difference.

Private Citizen:

1. <http://aww.uscg.mil>
2. <http://www.dhs.gov/how-do-i/report-suspicious-activity>

MTSA Regulated Facility Personnel:

33 CFR 101.305 Reporting.

(a) Notification of suspicious activities. An owner or operator required to have a security plan under part 104, 105, or 106 of this subchapter shall, without delay, report activities that may result in a transportation security incident to the National Response Center at the following toll free telephone: 1-800-424-8802, direct telephone 202-267-2675, or TDD 202-267-4477. Any other person or entity is also encouraged to report activities that may result in a transportation security incident to the National Response Center.

(b) Notification of breaches of security. An owner or operator required to have a security plan under parts 104, 105, or 106 of this subchapter shall, without delay, report breaches of security to the National Response Center via one of the means listed in paragraph (a) of this section.

(c) Notification of transportation security incident (TSI).

(1) Any owner or operator required to have a security plan under part 104 or 105 of this subchapter shall, without delay, report a TSI to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

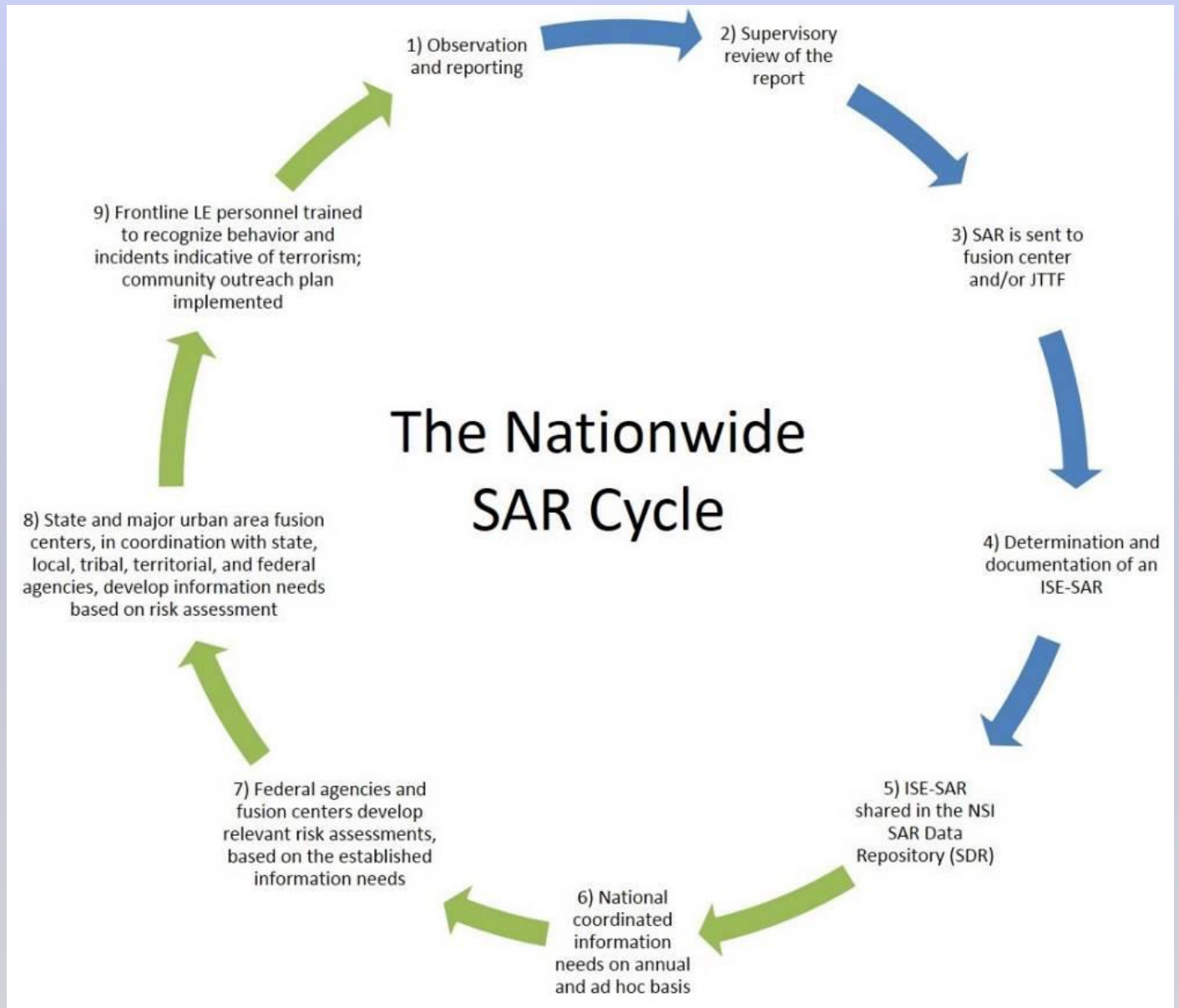
(2) Any owner or operator required to have a security plan under part 106 of this subchapter shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures

set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(d) Callers to the National Response Center should be prepared to provide as much of the following information as possible:

- (1) Their own name and contact information;
- (2) The name and contact information of the suspicious or responsible party;
- (3) The location of the incident, as specifically as possible; and
- (4) The description of the incident or activity involved.

If you are unsure, it is always the best to err on the side of caution and report something that seems out of the ordinary as suspicious activity. By working together, we can all do our part to ensure the safety and security of our ports.



https://nsi.ncirc.gov/documents/SAR_FS_1.5.5_PMISE.pdf

Continued on Page 4

SAR - Suspicious Activity Report

JTTF - Joint Terrorism Task Force

ISE-SAR - Information Sharing Environment-Suspicious Activity Report

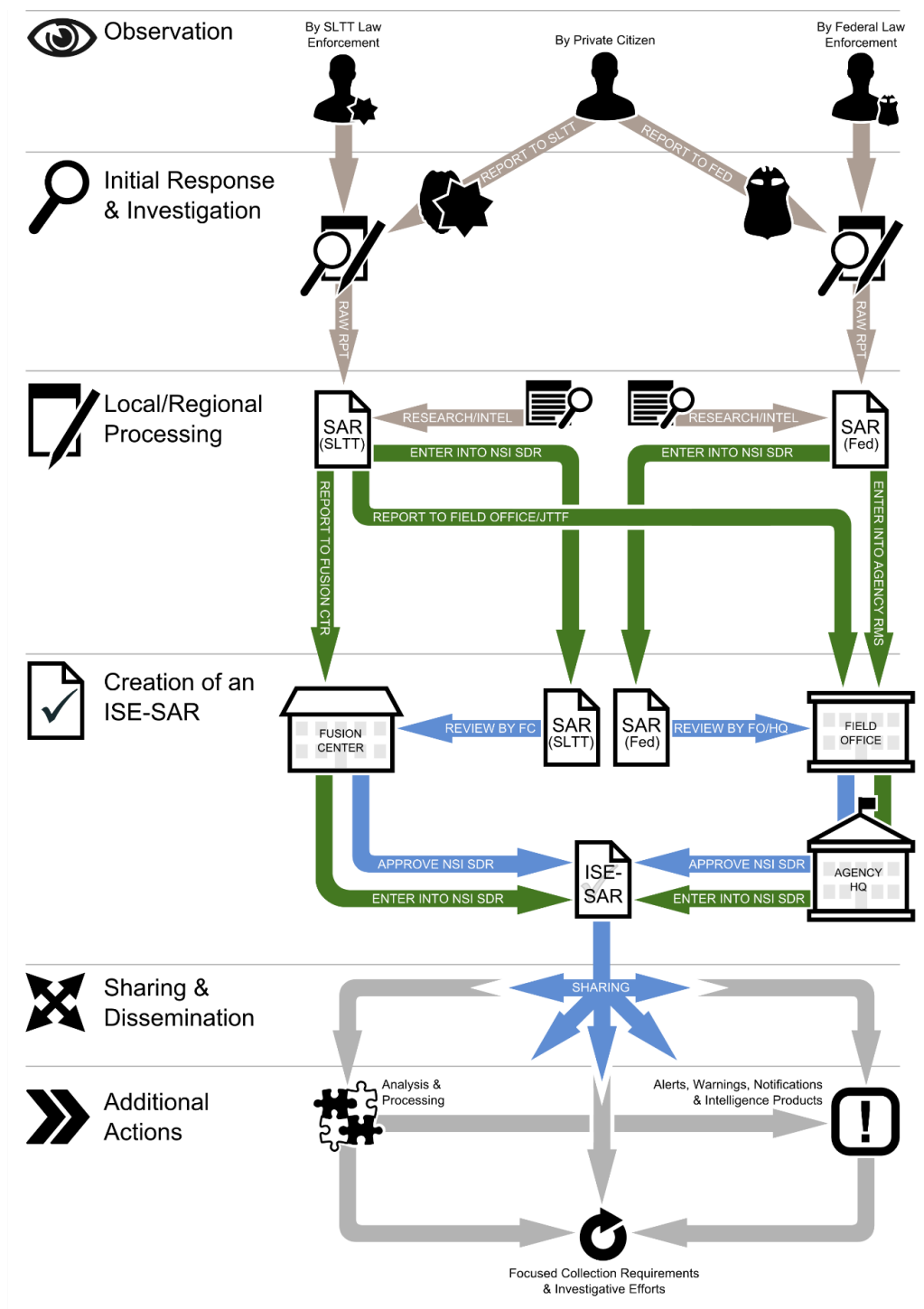
NSI - Nationwide SAR Initiative

LE – Law Enforcement

SLTT State, local, tribal, and territorial

SDR - Shared Data Repository

Fusion Center - serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners.





The Word in the Yard...

TRAINING

Next Resident Course

(Oklahoma), 21-25 March. Plenty of seats!

Exportable Courses include 7 remaining for FY16. Classes are **Houston** (Dec), **Honolulu** (Jan), **Charleston** (Feb), **Hampton Roads**, (Mar), **San Fran** (Apr), **New Orleans** (Apr) & **Boston** (Jun)

Exportable courses seat 20. They are for the area/unit AD, Reserves; All are no-cost orders.

DOD, CBP, NCB & AUX are welcomed

HIGH SECURITY SEALS UPDATE

Lack of seals is no longer a problem! From now through Dec., CITAT will be shipping out to units their CY16 seal allowance. New seals were bought by CG-FAC-2.

CITAT has reached out to container inspection units for seal needs. Please make sure you respond. Contact us via email, or call (405) 954-8985.

PERFORMANCE GOAL CALCULATOR (PGC)

COTP Zone: Savannah		CY 2014 Goal: 1535
Enter Annual Container Throughput in Boxes - Use data from your ports. If no data exists, use the throughput data from Table 1 on the right.		
1857748		
Qualify for National Cargo Bureau Incentive? (Click on cell to toggle Yes/No)	Yes	Table 1 Throughput Sector Anchorage 274425 Sector Baltimore 402311 MSU Baton Rouge 1482 Sector Boston 110875 Sector Charleston 798879 Sector Delaware Bay 116253 MSU Texas City (Galveston) 15517 Sector Guam 108634 Sector Hampton Roads 1102051 Sector Honolulu 497008 Sector Houston 1141763 Sector Jacksonville 466834 MSU Lake Charles 1609 Sector LA/LB 814739 Sector Miami 1199892 Sector Mobile 237278 Sector New Orleans 293293 Sector New York 1297016 Sector North Carolina 157867 Sector Northern New England 3426 MSU Port Arthur 3613 MSU Portland (Columbia River) 112000 Sector Puget Sound 1981396 Sector St. Petersburg 12227
Qualify for Customs and Border Patrol Incentive? (Click on cell to toggle Yes/No)	Yes	
Qualify for Port / Facility Incentive? (Click on cell to toggle Yes/No)	Yes	
Select the Confidence Interval (CI) Base by using the drop down list (click on cell) after comparing your throughput value to Table 2 below.	1.75	
Calculated Annual Performance Goal	1535	
Table 2		
COTP Throughput Threshold	Minimum CI	
Equal or greater than 5000000	0.5	
Equal or greater than 1000000	1.25	
Equal or greater than 300000	1.75	
Equal or greater than 100000	2.75	
Equal or greater than 50000	3.75	
Less than 50000	2	

Based on NCIP policy, all units should be using the PGC to determine container goal inspection numbers for the year. How many unit's use the PGC & set goals? And send the data to CG-FAC-2 by 1 Feb annually? Not all.

The PGC is a good tool. CITAT is emphasizing use of it. We will be reaching out to units on this topic.

But we also recognize the PGC could be improved upon. There is opportunity to add more "buy downs" such as for busy refrigerated or empty container traffic. The key is box count, not TEU. Box count is roughly 1/2 of TEU throughput. Buy-down credit is also key to lower your inspection numbers for the year. Each unit should use the latest data for their port to set actionable goals and not use the outdated/given PGC Table 1 data. Table 1 data will be updated soon.

At CITAT, we want to support NCIP inspection goals, with a focus on quality declared & undeclared hazmat inspections. CG-FAC-2 looks at the NCIP data & how units are performing. Between Sector Staffing Model, MISLE & PGC data, CG-FAC-2 determines a unit's ideal staffing number (increase or decrease staffing) and the health of the NCIP.

FYI: Go to the AAPA website (<http://www.aapa-ports.org/>) & select "Port Industry Info" then "Statistics" to see CY14 data for your port.

PHMSA: 2015 FINAL RULE REMINDER

In Jan 2015, PHMSA amended the 49 CFR HMR to align with IMDG by incorporating new amendments, including changes to proper shipping name, hazard classes, packing groups, special provisions, packaging & vessel stowage. Recent changes include:

- Adopting an exception from the HMR for Marine Pollutants up to 5 L (1.3 gal) for liquids or 5 kg (11 lbs.); for solids when these materials are packaged IAW the general packaging req's of § 173.24. And modifying the list of MPs in App'n'dx B to § 172.101.
- Revising/adding vessel stowage codes listed in column 10B of the HMT & segregation requirements in § 176.83 consistent with IMDG.
- Adding minimum sizes for overpack markings. And, amending the HMR definition of non-bulk packaging by adding new info to include bags & boxes, conforming to the applicable req's for spec packaging in §178, if they have a max net mass of 400 kg (882 pounds) or less.

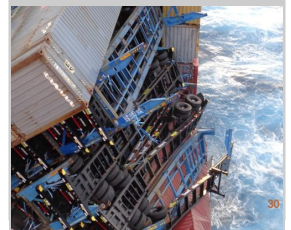
Read more at: <http://phmsa.dot.gov/hazmat/regs/rulemaking/archive>

CITAT UPDATE

After 21 years in Oklahoma, CITAT will move to Yorktown in 2017. Moving will align CITAT with the other marine safety courses.

Photo of the Month

From: Sector Baltimore



DID YOU KNOW?

Container shipping has doubled every 7 years since 2000, from 5 million TEU to **20 million TEU** in 2015.

MASFO FYI

CITAT recently supported Sector New Orleans and Sector Puget Sound MASFOs. CITAT plans to attend one MASFO per quarter. **Invite us. We're ready to help!**

As per the NCIP, COTPs with >500K TEU per year **shall** lead at least one MASFO per CY. All container units should strive to do one MASFO per year.

More on MASFOs next month's newsletter!

Have a topic you would like to see covered? Got a question? Email us at CITAT: CGI-PF-CITAT_MSG@uscg.mil or call us at (405) 954-8985.

Report to Congress on the "Strategy for Waterside Security of Especially Hazardous Cargo" has been signed by the Commandant and delivered to Congress

by Bob Reimann

Meeting 2010 CG Authorization Act requirements

The "Strategy for the Waterside Security of Especially Hazardous Cargo" was signed by Commandant Paul F. Zukunft on 1 September 2015. The report responds to Section 812 of the Coast Guard Authorization Act of 2010, which directs the Coast Guard to develop a strategy for the waterside security of vessels carrying and waterfront facilities handling, especially hazardous cargo. The strategy utilizes the results of the May 14, 2012, "Waterside Security of Especially Hazardous Cargo National Study Results." The Strategy for the Waterside Security of Especially Hazardous Cargo establishes the framework by which the federal government, led by the Department of Homeland Security, addresses risks to the Marine Transportation System posed by a waterside attack or other maritime incident causing a release involving Especially Hazardous Cargoes.



Background and Cargoes

Especially Hazardous Cargoes (a subset of Certain Dangerous Cargoes (CDC's) consisting of **Anhydrous Ammonia** (NH_3), **Ammonium Nitrate** ($\text{NH}_4(\text{NO}_3)$), **Chlorine** (Cl_2), **LNG** (predominantly methane, CH_4) & **LPG** (propane or butane)) flow through U.S. ports and waterways on a daily basis. The potential for release and subsequent reactivity of these cargoes along with their normal transport in close proximity to high density population areas and critical infrastructure was one of the main reasons for having this holistic strategy in place to mitigate the associated risks. Current security posture and concomitant Coast Guard resources employed during the transit of EHC laden vessels are determined by the Captain of the Port (COTP) working with appropriate local port stakeholders. As the public and political awareness of EHC increases, our finite resources must be



logically applied to address the emerging concerns and increased visibility factor placed upon the movement of commodities through our ports. In order to ensure optimal balance and to increase the level of standardization of methodology throughout the field, the Coast Guard must develop and execute an Implementation Plan that will build upon the solid foundation of previous efforts to enhance coordination with our port partners and encourage their efforts to reduce waterside vulnerabilities associated with these cargoes. The securing and safeguarding of EHCs will support reliable movement of these cargoes within our domestic borders and will reduce the risk of disruption to our waterways.

Stakeholder Linkage

There are currently several CGHQ offices that have responsibilities associated with the movement of CDC's/EHC's in bulk. The first step en route to developing an implementation plan will be to establish a functioning risk reduction workgroup consisting of those offices having equity from both a safety and security perspective. This will create a concentrated level of subject matter expertise upon which to guide the formulation of the implementation plan.

Third Party Analysis

In order to understand the full range of our existing activities and shortfalls while avoiding the potential for skewing the results, a third party will provide a detailed analysis of the individual activities conducted by the offices comprising the risk reduction workgroup. The objective will be to highlight current efforts and outline existing gaps. Deliverables of the report required of the workgroup will be in the form of recommendations as how to improve our internal processes and the logical linkage to external agencies and their activities related to risk mitigation of EHC's.

An additional portion of the analysis will consist of a review of existing studies related to CDC's/EHC's as well as ongoing technology based research & development projects. One of the deliverables will be determining if the existing data that has been compiled is sufficient and if it will serve as an exceptional foundation or if further studies need to be undertaken to bridge informational gaps. Upon the completion of both phases of the analysis, the workgroup will analyze the data and take the appropriate actions as per the recommendations offered in the final report coming out of the workgroup.

Implementation Plan will be a “living” document

Although the likelihood of an attack or other incident that creates a release is low, a successful attack on the nation's Marine Transportation System, especially where it involves EHCs, could cause significant injury and loss of life, as well as damage to critical infrastructure and key resources. The high consequence nature of such an incident underscores the importance of developing, implementing, maintaining, and periodically reviewing and modifying existing security and safety policies, as well as requirements to address EHCs. Responsibility for waterside security of EHCs is shared between facility and vessel masters, owners, operators and agents, as well as DHS and its partners in the private and public sectors. DHS has taken an approach incorporating especially hazardous cargoes as part of a larger all-hazards protection scheme.

The Strategy articulates a framework which incorporates EHCs into DHS' all hazards risk assessment and mitigation processes. The Coast Guard will lead efforts to implement this strategy, employing existing authorities, regulatory requirements, and voluntary standards. In addition, the strategy is modeled after certain tenets of the President's Executive Order 13650, Improving Chemical Facility Safety and Security, including information sharing and collaboration with state, tribal and local partners. The resulting Implementation Plan will be a living document intended to be continually updated.

Detailed versions with content appropriate to federal program planning and management will be maintained within Coast Guard. Stand by to be informed on future bulk chemical security issues by CG-FAC.



CYBER TIME!

By LT Josephine Long

Since the Cyber Strategy was signed last June, many inspectors are eager to start dialogue with facility owners and operators on how this will impact the industry in the future. We encourage inspectors to discuss cyber with their industry representatives, and to point them towards our cyber security page on Homeport (in the Missions Tab) for additional resources, news on cyber, and other cyber information.

As part of these conversations, inspectors should make it clear we do not require them to include cyber in their security plans at this time. If the facility wishes to include cyber on a voluntary basis, we ask the units to contact our office to advise the owners and operators on how this would be best accomplished. We encourage inspectors to concentrate on raising awareness, info sharing and educating industry about available resources.

Both LANTAREA and PACAREA have conducted train-the-trainer programs with the expectation that every unit gives awareness training to targeted personnel within their units by March 1, 2016. Our goal

is to ensure industry representatives understand that the Coast Guard views cyber as a legitimate safety, security and operational risk for the marine transportation system, but that we are still working on a policy on how to incorporate cyber into our safety and safety programs.



Please contact LCDR Joshua Rose at Joshua.D.Rose@USCG.Mil or LT Josephine Long at Josephine.A.Long@USCG.mil with any questions.

DATE STAMPING FACILITY SECURITY PLANS

By LCDR Jennifer Osburn

Did you know that during FORCECOM's Mission Management System (MMS) Audits, the Facility Inspection Program's number one deficiency is Facility Security Plans (FSP) not being date stamped? This requirement can be found in Navigation and Inspection Circular (NVIC) 03-03, Change 2, Enclosure 1 (specifically 1.3.1).

The purpose of this requirement is to ensure adequate document version control throughout the FSP approval process, and to track the review process timeline.

Additionally, it provides documentation to compare the date of receipt to the expiration date of the previously approved FSP. Please ensure you date stamp all FSPs upon receiving them, even if it is a resubmission.

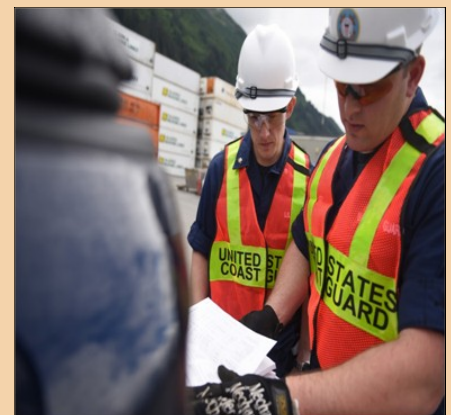
If you have any questions, or are unable to purchase a date stamp, please do not hesitate to contact us at (202) 372-1132.



CONTAINER GOAL CALCULATOR for 2016

CG-FAC would like to put out a reminder to all applicable units that the Container Inspection programs need to send in the annual throughput numbers into CG-FAC-2 as per COMDTINST 16616.11 National Container Inspection Program. These numbers assist in updating the performance goal calculator for each port, updated throughput numbers should be sent to the following email address:

FAC-2-SAFETY@uscg.mil. For any future safety questions in regards to Containers, Explosive Handling or regulated Facilities, they should be sent to FAC's new email address at FAC-2-SAFETY@uscg.mil.



Chemical Facility Anti-Terrorism Standards (CFATS)

What does this mean to me?

by LCDR Jennifer Osburn & LCDR Derrick Saunders

Chemicals are vital to our national economy. They are used in manufacturing microprocessors, in research at universities, and even at vineyards. When used properly, chemicals better our lives. However, in the wrong hands, some chemicals can also be used for great harm.

The Infrastructure Security Compliance Division (ISCD) within the National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection, is the division within the Department of Homeland Security (DHS) that is responsible for administering the CFATS program. The objective of CFATS is to identify and regulate high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with dangerous chemicals. The regulatory authority for this program is contained in part 27 of title 6 of the Code of Federal Regulations. Any facility that manufactures, uses, stores, or distributes certain chemicals above a specified quantity listed in an appendix to the regulation (Appendix A) has to complete a preliminary risk assessment using the Department's Chemical Security Assessment Tool. Facilities covered may include, among other types of facilities, universities, hospitals, warehouses and distributors, refineries, and chemical manufacturing facilities. Facilities, or portions of facilities, subject to MTSA are statutorily exempt from CFATS.

Facilities determined to be high-risk by ISCD are then required to develop and implement a security site plan that address 18 individual Risk Based Performance Standards. CFATS field inspectors visit the facilities for an authorization inspection as well as follow-on compliance inspections.

The U. S. Coast Guard (USCG) and NPPD are key partners in the protection of critical infrastructure across the nation. Over the past several years, the USCG and NPPD have been formally collaborating through a national working group, which is co-chaired by CG-FAC and ISCD. Currently a Coast Guard liaison is detailed from CG-FAC to ISCD, LCDR Derrick Saunders. He has been working on initiatives to ensure coordination and awareness between the MTSA and CFATS programs, as well as introduce field inspectors from both programs via outreach and cross training. LCDR Saunders and two other members of CG-FAC recently completed inspections training with CFATS field inspectors, which covered RBPS-8 (Cyber). The three day training session focused on a cyber system overview, how it works, questions to ask facility employees about their cyber systems, procedures, and vulnerabilities, and what to look for during inspections.

For additional information about the CFATS program, please visit <http://www.dhs.gov/chemical-facility-anti-terrorism-standards>, or contact either LCDR Derrick Saunders at derrick.saunders@hq.dhs.gov or LCDR Jennifer Osburn at jennifer.m.osburn@uscg.mil. Documents comparing MTSA and CFATS can be found on CG-FAC's portal page.

LCDR Jennifer Osburn, LT Josie Long & LCDR Derrick Saunders with members of ISCD at the CFATS Cyber Inspections training.



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 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, & 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 202-372-1136
 LT Bill Gasperetti 202-372-1139

Security Standards (Regulation Development)

LCDR Kevin McDonald 202-372-1168
 LT Cal Fless 202-372-1151

Strategic Planning Initiatives

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/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>